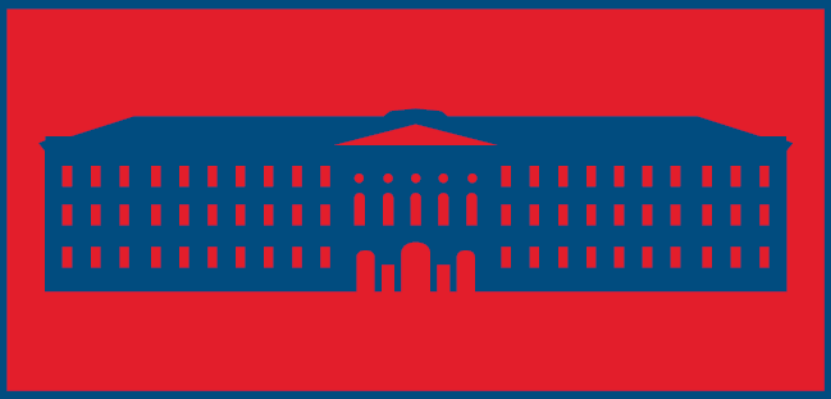
Berzsenyi Dániel
Gyaraki Réka
Hámornik Balázs Péter
Hirsch Gábor
Kiss Attila
Marsi Tamás
Orbók Ákos
Simon Béla
Solymos Ákos
Tikos Anita
Zsíros Péter

Incidensmenedzsment



Dialóg Campus

Berzsenyi Dániel – Gyaraki Réka – Hámornik Balázs Péter – Hirsch Gábor – Kiss Attila – Marsi Tamás – Orbók Ákos – Simon Béla – Solymos Ákos – Tikos Anita – Zsíros Péter

INCIDENSMENEDZSMENT

Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2017

Dialóg Campus Kiadó ❖ Budapest

A kiadvány a KÖFOP-2.1.1-VEKOP-15-2016-00001 „A közszolgáltatás komplex kompetencia, életpálya-program és oktatás technológiai fejlesztése” című projekt keretében jelent meg.

Szerzők:
Berzsenyi Dániel
Dr. Gyaraki Réka
Dr. Hámornik Balázs Péter
Hirsch Gábor
Dr. Kiss Attila
Marsi Tamás
Orbók Ákos
Dr. Simon Béla
Solymos Ákos
Tikos Anita
Zsíros Péter

Szakmai lektor:
Dr. Krasznay Csaba

TARTALOM

1. Berzsenyi Dániel: A KIBERTÉR AKTUÁLIS NEMZETKÖZI BIZTONSÁGPOLITIKAI KIHÍVÁSAI 9
1.1. Bevezetés 9
1.2. Biztonsági trendek a kibertérben 10
1.3. A lokális folyamatokat érintő kiberbiztonsági kihívások 13
1.4. A regionális folyamatokat érintő kiberbiztonsági kihívások 14
1.5. A globális folyamatokat érintő kiberbiztonsági kihívások 17
1.6. Kiberbiztonság a nemzetközi béke és biztonság tükrében 24

2. Dr. Kiss Attila: A BIZTONSÁGI ESEMÉNYEK ÉS AZ ADATVÉDELMI INCIDENSEK KEZELÉSÉRE VONATKOZÓ ELŐÍRÁSOK HAZÁNK ÉS AZ EU JOGÁBAN 27
2.1. A biztonsági események jogi jelentősége 27
2.1.1. Bevezető gondolatok 27
2.1.2. A kapcsolódó fogalmak áttekintése 28
2.1.3. A biztonsági esemény tulajdonságai 30
2.1.4. Az események kezelésére vonatkozó előírások 32
2.1.4.1. Az Ibtv. által rögzített feladatok 32
2.1.4.2. Intézkedések meghatározott osztályok alapján 32
2.1.4.3. A 3. biztonsági osztálytól kötelező intézkedések köre 33
2.1.4.4. A 4. biztonsági osztálytól kötelező intézkedések köre 34
2.1.4.5. Az 5. biztonsági osztálytól kötelező intézkedések köre 34
2.1.5. A BM rendelet 4. melléklete szerinti védelmi intézkedési katalógus 35
2.1.6. Az eseménykezelés nemzeti intézményrendszere 35
2.1.7. Adatvédelem, adatbiztonság és információbiztonság 37
2.1.8. Adatvédelmi incidensek nyilvántartási és bejelentési kötelezettsége 2018-ig 38
2.1.9. Az Európai Digitális Menetrend 2014–2020 céljai 40
2.1.10. Eseménykezelési elvárások a GDPR szabályozásában 40
2.1.10.1. A GDPR viszonya a hatályos adatvédelmi előírásokhoz 40
2.1.10.2. A GDPR adatbiztonsági rendelkezései és incidenskezelésre vonatkozó előírásai 41
2.1.10.3. Gyakorlati kérdések és aggályok a GDPR előírásainak alkalmazhatósága kapcsán 43
2.1.11. Eseménykezelés a NIS irányelv alapján 44
2.1.11.1. Út az irányelv megszületéséig 44
2.1.11.2. A NIS irányelv 45
2.1.11.3. Eseménykezelés és bejelentési kötelezettség a NIS alapján 46

3. Marsi Tamás: A NEMZETI KIBERVÉDELMI INTÉZET SZEREPE AZ ESEMÉNYKEZELÉSBEN 49
3.1. A Nemzeti Kibervédelmi Intézet és szerepe az eseménykezelésben, valamint a sérülékenységvizsgálati tevékenységben 49
3.1.1. A kibertér és fenyegetései 49
3.1.2. A Nemzeti Kibervédelmi Intézet 50
3.1.2.1. Történet és megalakulás 50
3.1.2.2. Az intézet felépítése, jogszabályi háttere 51
3.1.3. A Kormányzati Eseménykezelő Központ 51
3.1.3.1. A GovCERT feladat- és hatásköre 51
3.1.3.2. A GovCERT ügyfelei és partnerei 52
3.1.4. A fenyegetettségmenedzsment 53
3.1.4.1. A fenyegetésekről általában 53
3.1.4.2. A fenyegetettségmenedzsment folyamata 54

3.1.4.3. A fenyegetettségmenedzsment bemenete 55
3.1.4.4. A fenyegetettségmenedzsment kimenete, termékei 56
3.1.5. A biztonsági események kezelése 57
3.1.5.1. A biztonsági eseménnyel kapcsolatos alapfogalmak 57
3.1.5.2. A biztonsági események kezelésének alapszabályai 59
3.1.5.3. Biztonsági események keletkezése 60
3.1.5.4. A biztonsági események feldolgozása, elővizsgálata 61
3.1.5.5. A biztonsági események koordinálása 63
3.1.5.6. A biztonsági események részletes technikai vizsgálata 64
3.1.5.7. A biztonsági események lezárása 65
3.1.5.8. A biztonsági események utóélete 66
3.1.5.9. Gyakorlati tapasztalatok 67
3.1.5.10. Intézkedési terv az NKI-val közös incidenskezelésre 67
3.1.5.11. Incidenskezelés a gyakorlatban 68
3.1.6. Sérülékenységvizsgálat 71
3.1.6.1. Sérülékenységvizsgálati tevékenység 72
3.1.6.2. A sérülékenységvizsgálati projekt kezdete 73
3.1.6.3. A sérülékenységvizsgálat lefolyása 75
3.1.6.4. A sérülékenységvizsgálat lezárása 77
3.1.6.4. A sérülékenységvizsgálat egyéb szabályai 77
3.1.7. A GovCERT támogató és koordinációs feladatai 78
3.1.7.1. Tudatosító tevékenység 78
3.1.7.2. Technikai tanácsadás 79
3.1.7.3. Kibervédelmi gyakorlatok 79
3.1.7.4. Kiberbiztonsági koordináció és nemzetközi szerepvállalás 79
3.1.8. Hatósági tevékenység 79
3.1.8.1. A hatósággal kapcsolatos alapfogalmak 80
3.1.8.2. A hatóság által kezelt adatok 80
3.1.8.3. Ügytípusok 81
3.1.8.4. A hatóság további jogkörei és feladatai 82
3.1.8.5. A GovCERT és a hatóság elhatárolása 82
3.1.9. Biztonságirányítás 83
3.1.9.1. A védett rendszerek 83

4. Tikos Anita: BIZTONSÁGI ESEMÉNYKEZELÉS A NEMZETKÖZI TÉRBEN – A CERT/CSIRT MŰKÖDÉSE 85
4.1. A CERT és a CSIRT fogalma 85
4.1.1. Kialakulása 86
4.1.2. CSIRT-típusok 87
4.2. A CSIRT-ek feladatai, szolgáltatásai 89
4.2.1. Válaszintézkedést nyújtó szolgáltatások (reaktív szolgáltatások) 89
4.2.2. Megelőző szolgáltatások 91
4.2.3. Biztonságkezelési és minőségirányítási szolgáltatások 92
4.2.4. Az európai uniós szabályozás által definiált CSIRT-feladatok 93
4.3. Az incidenskezelés hátterének megismerése 94
4.3.1. Az ENISA 94
4.3.2. Az Information Technology Infrastructure Library (ITIL) 95
4.3.3. A Control Objectives for Information and Related Technologies (Cobit) 95
4.3.4. National Institute of Standards and Technology (NIST) 95
4.3.5. Az ISO 27000-es szabványcsalád 95
4.3.6. Jogalkotás 95
4.4. A CSIRT-ek Magyarországon 96
4.4.1. A Kormányzati Eseménykezelő Központ 96
4.4.2. Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja 97
4.4.3. A honvédelmi ágazat CERT-je: a Military CERT (MilCERT) 98
4.4.4. A Hun-CERT 98
4.4.5. NIIF-CSIRT 98
4.5. Nemzetközi együttműködés 98

4.5.1. Az együttműködések jogi formája, szabályai 99
4.5.2. A közösségek tagsági szabályai 99
4.5.3. Nemzetközi közösségek 100
4.5.3.1. Forum of Incident Response and Security Teams (FIRST) 100
4.5.3.2. Internet Watch and Warning Network (IWWN) 100
4.5.3.3. Európai közösségek 100
4.5.3.4. Regionális együttműködések 102
4.5.3.5. Information Sharing and Analysis Centers 102
4.6. CSIRT létrehozása 103

5. Dr. Hámornik Balázs Péter – Orbók Ákos: BIZTONSÁGI MŰVELETI KÖZPONTOK (SOC-K) 110
5.1. Bevezető 110
5.2. A biztonsági műveleti központok fogalma és modelljei 111
5.3. A működéshez lényeges képességek, szakértelem – és a szakemberek megtartása 112
5.3.1. A biztonsági események és az információ kezelésének kritikus képességei 113
5.3.2. A SOC tervezésének, megvalósításának, üzemeltetésének és fejlesztésének kulcskérdései 113
5.3.3. Előkészítés 114
5.3.4. Tervezés 115
5.3.5. A SOC megvalósítása 117
5.3.5.1. A rálátást, láthatóságot biztosító eszközök 118
5.3.5.2. Elemző eszközök 118
5.3.5.3. Cselekvést és menedzsmentet lehetővé tevő eszközök 119
5.3.5.4. A SOC üzemeltetése 120
5.3.5.5. A SOC fejlesztése és bővítése 122
5.4. A TI-vezérelt biztonsági műveleti központ jellemzői 125
5.5. A SIEM-ek szerepe a SOC-kban 126
5.5.1. Naplófájlok (logok) 126
5.5.2. Emberi tényezők a SIEM üzemeltetésében 128
5.5.3. A SIEM működése 128
5.5.4. A SIEM-piac szereplői 130
5.6. A SIEM alkalmazása a célzott támadásészlelésre 132
5.7. Megoldások a SOC házon belüli megvalósításának lehetetlensége esetén 133
5.8. sszegzés 135

6. Hirsch Gábor: AZ ESEMÉNYKEZELÉS MŰSZAKI ESZKÖZTÁRA – REFERENCIAARCHITEKTÚRA 136
6.1. Az eseménykezelés műszaki eszköztára – referenciaarchitektúra 136
6.1.1. Bevezetés 136
6.1.2. Az incidenskezelés lépései 136
6.1.2.1. Identify 138
6.1.2.2. Protect 139
6.1.2.3. Detect 142
6.1.2.4. Respond 143
6.1.2.5. Recover 144
6.1.3. Referenciaarchitektra kis szervezetek számára 146
6.1.4. Referenciaarchitektra közepes szervezetek számára 148
6.1.5. Referenciaarchitektra nagy szervezetek számára 150
6.1.6. SIEM, Cyber Threat Intelligence, SOC 154
6.1.7. Magyaroszágon elérhető biztonsági gyártók, megoldásaik és kiválasztásuk 156
6.1.7.1. Műszaki alkalmassági szempontok 156
6.1.7.2. Gazdasági szempontok 157
6.1.7.3. Közbeszerzési szempontok 157
6.1.8. Megfelelés az Ibtv. követelményeinek 158
6.1.9. sszefoglaló 160

7. Solymos Ákos – CISM – CRISC: A SZERVEZETEN BELÜLI INCIDENSKEZELÉSI GYAKORLATOK SZERVEZÉSE 161
7.1. Végfelhasználói feladatok az incidenskezelésben 161
7.1.1. PPT – People, Process, Technology 162

7.1.1.1. People 162
7.1.1.2. Process 165
7.1.1.3. Technology 167
7.1.1.4. PPT, a háromlábú szék 168
7.1.2. Biztonságtudatosság és kockázatérzékenység mint gondolkodásmód kialakítása 169
7.1.3. A kockázatérzékenységnek és a biztonságtudatosságnak mint a szervezeti kultúra részeinek kialakítása a szervezetben 170
7.1.3.1. Biztonsági politika, információbiztonsági politika, vezetői felelősségvállalás 171
7.1.3.2. Kockázatmenedzsment mint a szervezeti biztonságtudatosság mozgatórugója 171
7.1.3.3. Következménymenedzsment mint a kockázatmenedzsment mozgatórugója 171
7.1.4. Az oktatás és a tudatosítás megjelenése a vonatkozó hazai jogszabályokban és a nemzetközi szabványokban 172
7.1.4.1. ITB ajánlások 172
7.1.4.2. Közigazgatási informatikai bizottság 25. számot viselő ajánlássorozata 173
7.1.4.3. A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 173
7.1.4.4. A 41/2015. (VII. 15.) BM rendelet 174
7.1.4.5. MSZ/T ISO/IEC 27001:2014 177
7.1.5. Az incidenskezelés folyamata és szakaszai 178
7.1.5.1. Végfelhasználói feladatok az incidens előtt 179
7.1.5.2. Végfelhasználói feladatok az incidens alatt 180
7.1.5.3. Végfelhasználói feladatok az incidens után 181
7.1.5.4. Az incidenskommunikáció és az incidensjelentési csatornák 181
7.1.6. Incidenskezelési tervek 182
7.1.6.1. Incidenskezelési gyakorlatok 182
7.1.6.2. Az incidenskezelési gyakorlatok tervezése 182
7.1.6.3. Az incidenskezelési gyakorlatok típusai 182
7.1.6.4. A tesztelés lebonyolítása 184
7.1.6.5. A teszt kiértékelése (lessons learned) 185
7.2. Az incidenskezelés bemutatása a tudatossági oktatásokban 185
7.2.1. A biztonsági oktatások és a tudatossági kampányok végrehajtásának előnyei 185
7.2.2. Eszközök a munkavállalók figyelmének felkeltésére, fenntartására; motiváció, buy-in, lessons learned 186
7.2.3. A tudatosságépítés folyamata, motivációk, figyelemfenntartás 187
7.2.4. A biztonsági oktatás és a tudatossági kampány közti különbségek 187
7.2.5. A biztonságtudatossági kampányok tervezése, előkészítése és végrehajtása 188
7.2.5.1. A biztonságtudatossági kampány emberi erőforrásigénye 188
7.2.5.2. A pénzügyi tervezés 189
7.2.5.3. A szakmai tervezés 190
7.2.5.4. Megvalósítás 190
7.2.5.5. Visszamérés 190
7.2.6. A biztonsági oktatások tervezése, előkészítése és végrehajtása 190
7.3. Példák az incidenskezelés bemutatására, végfelhasználók számára 191
7.3.1. Az adathalászat elhárítása 191
7.3.1.1. Az incidens előtti tevékenységek 191
7.3.1.2. Az incidens alatti tevékenységek 192
7.3.1.3. Az incidens utáni tevékenységek 194
7.3.2. A vírusvédelmi incidens elhárítása 194
7.3.2.1. Az incidens előtti tevékenységek 194
7.3.2.2. Az incidens alatti tevékenységek 195
7.3.2.3. Az incidens utáni tevékenységek 195

8. Dr. Gyaraki Réka – Dr. Simon Béla: BIZTONSÁGI ESEMÉNYEK RENDÉSZETI SZEMPONTBÓL – A KIBERBŰNCSELEKMÉNYEK KEZELÉSE 197
8.1. Biztonsági események rendészeti szempontból – a kiberbűncselekmények kezelése 197
8.1.1. Az informatikához kapcsolódó bűncselekmények és azok kezelése Magyarországon 197
8.1.2. A kiberbűncselekmények jellemzői 199
8.1.3. A számítógépes bűncselekmények elkövetési területei 201
8.1.4. Az információcserére vonatkozó hazai és nemzetközi jogi szabályozások 202

8.1.5. A kiberbűncselekményekhez kapcsolható egyéb szervezetek 203
8.1.5.1. A Nemzetbiztonsági Szakszolgálat 203
8.1.5.2.A Nemzeti Kibervédelmi Intézet 204
8.1.5.3. Az Alkotmányvédelmi Hivatal 205
8.1.5.4. Az Információs Hivatal 205
8.1.5.5. A Katonai Nemzetbiztonsági Szakszolgálat 206
8.1.5.6. BM Országos Katasztrófavédelmi Főigazgatóság 207
8.1.5.7. A Terrorelhárítási Központ 208
8.1.6. Büntető törvénykönyvi tényállások 208
8.1.6.1. Btk. 375. § Információs rendszer felhasználásával elkövetett csalás 208
8.1.6.2. Btk. 423. § információs rendszer vagy adat megsértése 209
8.1.6.3. Btk. 424. § információs rendszer védelmét biztosító technikai intézkedés kijátszása 212
8.1.6.4. Btk. 204. § gyermekpornográfia 213
8.1.6.5. Btk. 385. § szerzői vagy szerzői joghoz kapcsolódó jogok megsértése 213
8.1.6.6. Btk. 386. § védelmet biztosító műszaki intézkedés kijátszása 214
8.1.7. A büntetőeljárásra vonatkozó egyes szabályok 214
8.1.7.1. Megkeresések 214
8.1.7.2. A lefoglalás 215
8.1.7.3. A házkutatás 218
8.1.7.4. Az információs rendszerben tárolt adatok megőrzésére kötelezés 220
8.1.7.5. Az elektronikus hírközlő hálózat útján közzétett adatok ideiglenes hozzáférhetetlenné tétele 222
8.1.7.6. Kapcsolódó büntető törvénykönyvi rendelkezések 224
8.1.7.7. Az elektronikus adat végleges hozzáférhetetlenné tétele 225
8.1.8. Nemzetközi rendészeti együttműködés a kiberbűnözés területén 225
8.1.8.1. Az Egyesült Nemzetek Szervezete (ENSZ) 226
8.1.8.2. Gazdasági Együttműködési és Fejlesztési Szervezet (OECD): 226
8.1.8.3. Az Európa Tanács (ET) 227
8.1.8.4. Az Európai Tanács 228
8.1.8.5. Az Európai Unió Belső Biztonsági Állandó Bizottsága (COSI) 228
8.1.8.6. Az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) 229
8.1.8.7. Az Europol 230
8.1.8.8. A Kooperatív Kibervédelmi Kiválósági Központ (Cooperative Cyber Defence Centre of Excellence – CCD COE) 233
8.1.8.9. Cyber Defence Management Authority – CDMA 233
8.1.8.10. Computer Emergency Response Teamek (CERT) 233
8.1.8.11. International Telecommunications Union (ITU) 233
8.1.8.12. Az Európai Kiberbűnözés Elleni Akciócsoport (European Cyber Crime Task Force) 234
8.1.8.13. Európai Multidiszciplinárius Platform a Bűnügyi Fenyegetés Ellen (European Multidisciplinary Platform Against Criminal Threats) 234
8.1.8.14. Eurojust 235
8.1.8.15. Az Interpol 235

9. Zsíros Péter: BIZONYÍTÉKSZERZÉS AZ INFORMATIKAI RENDSZEREKBŐL 236
9.1.Bevezetés 236
9.1.1. A legfontosabb szabályok, amelyeket be kell tartani 236
9.1.2. A vizsgálat főbb lépései 237
9.2. Lefoglalás (Acquire) 238
9.2.1. Szükséges eszközök 238
9.2.2. A memóriatartalom mentése 239
9.2.2.1. Windowsos gép memóriatartalmának mentése DumpIt alkalmazással 240
9.2.2.2. Windowsos gép memóriatartalmának mentése Winpmem 1.6.2 alkalmazással 243
9.2.2.3. Windowsos gép memóriatartalmának mentése Winpmem 2.1 alkalmazással 244
9.2.2.4. Windowsos gép memóriatartalmának mentése FTK imager alkalmazással 245
9.2.2.5. Windowsos gép memóriatartalmának mentése OSF programmal 248
*9.2.2.6. *Nix alapú gép memóriatartalmának mentése* 251

*9.2.2.7. *Nix alapú gép memóriatartalmának mentése Fmem és Forensics Memory eszközökkel* 251
*9.2.2.8. *Nix alapú gép memória tartalmának mentése LiMe és Linux Memory Extractor eszközökkel* 251
9.2.3. Másolat készítése az adathordozóról 258
9.2.4. Disk Image készítése futó számítógépről 260
9.2.4.1. Windows alapú gép 260
9.2.4.2. Másolat készítése az FTK imager alkalmazással 263
9.2.4.3. Másolat készítése az OSF alkalmazással 268
9.2.5. Disk image készítése kikapcsolt számítógépről 272
9.2.5.1. Másolatkészítés dd paranccsal 274
9.2.5.2. Másolatkészítés a dcfldd alkalmazással 276
9.2.5.3. Másolatkészítés ewfacquire alkalmazással 278
9.3. Memória Image vizsgálata 283
9.3.1. Volatility 283
9.4.1.1. Operációs rendszer verziójának megállapítása volatilityvel 284
9.4.1.2. A volatility helpje 284
9.4.1.3. A Truecrypt (veracrypt) kulcs megszerzése memóriadumpból 294
9.4.1.4. Rejtett process megtalálása memóriadumpból 294
9.4.1.5. A processek által használt erőforrások megtalálása 299
9.4.1.6. Processek által használt dll-ek megtalálása 299
9.4.1.7. A hálózati kapcsolatok kilistázása 300
9.3.2. Lostpassword 301
9.4.2.1. Truecrypttel (veracrypttel) titkosított disk kibontása 302
9.4.2.2. A bitlockerrel titkosított disk kibontása 306
9.4. A diskimage vizsgálata 309
9.4.1. Master Boot Record (MBR) 309
9.4.2. Guid Partition Table (GPT) 311
9.4.3. Volume Boot Record (VBR) 315
9.4.4. NTFS fájlrendszer 316
9.4.4.1. Standard Information Block 0x10 319
9.4.4.2. Filename Block 0x30 319
9.4.4.3. Data Block 0x80 Resident 320
9.4.4.4. Data block 0x80 Non-Resident 321
9.4.4.5. A cluster chain felépítése 322
9.4.4.6. CMEA idők használata 324
9.4.5. FAT fájlrendszer 326
9.4.6. Software reference library-k 330
9.4.7. Sleuthkit használata 331
9.4.8. Autopsy 334
9.4.9. Törölt fájl visszaállítása 341
9.5. A böngészőesemények vizsgálata 344
9.5.1. Az internet explorer 344
9.5.2. Firefox 347
9.5.3. Chrome 354
9.5.4. Flash 361
9.6. E-mailek vizsgálata 362
9.6.1. OST, PST fájlok 362
9.7. Logok vizsgálata 370
9.7.1. Windows operációs rendszerek logjai 370
9.7.2. A Linux operációs rendszer logjai 381
9.8. Egyéb bizonyítékforrások 384
9.8.1. Windows registry 384
9.8.2. Windows prefetch fájlok 386

JOGSZABÁLYTÁR 388

FOGALOMTÁR 391

1. A KIBERTÉR AKTUÁLIS NEMZETKÖZI BIZTONSÁGPOLITIKAI KIHÍVÁSAI

Berzsenyi Dániel

1.1. Bevezetés

Napjainkban egyre szélesebb körben ismert és elfogadott tény, hogy korunk biztonságpolitikai kihívásai között kiemelkedő szerepet töltenek be a kibertérből érkező kihívások, fenyegetések és veszélyek. Ennek legfőbb oka – számuk folyamatos növekedésén túl –, hogy a mindennapi életünk egyre több területén fejtenek ki egyre jelentősebb hatást, tehát a fenyegetési spektrum is dinamikusan növekszik. Miközben az információs társadalomban természetesnek vesszük, hogy a kibertérből elérhető adatok és információk száma folyamatos növekedést mutat, sokak számára kevésbé nyilvánvaló, hogy ezeknek a megfelelő szintű védelméről is gondoskodnunk kell. Tovább súlyosbítja a helyzetet, hogy az infokommunikációs technológia fejlődése következtében egyre több társadalmi folyamat zajlik a kibertérben vagy annak felhasználásával, és a folyamatosan gyarapodó információkhoz egyre többféle módon és egyre többféle eszközzel férhetünk hozzá.

Korábban egy átlagos felhasználó számára a legnagyobb problémát az jelentette, ha óvatlansága miatt számítógépe vírussal fertőződött meg, és ennek következtében kéretlen reklámüzeneteket kapott vagy átmenetileg blokkolták a hálózati hozzáférését. Idővel azonban kialakult egy olyan alapvető biztonságtudatosság, aminek köszönhetően ma már a legtöbb számítógépes felhasználó számára egyértelmű, hogy a megfelelő célszoftverekkel (víruskereső, tűzfal) jelentős mértékben csökkenteni tudja veszélyeztetettségét. Az elmúlt néhány évben viszont gyökeresen átalakult a kiberbiztonság helyzete nemcsak egyéni, de nemzeti, regionális és globális szinten egyaránt. A jelenleg is tartó átalakulás rendkívül gyorsan és komplex módon zajlik. A kibertérben elérhető szolgáltatások dinamikus bővülése, az okoseszközök rohamos elterjedése, a gyártók felelőtlensége, a rosszindulatú felhasználók és az általuk alkalmazott módszerek gyarapodása, valamint a technológiai és tudástranszfer következtében mára egy átlagos felhasználó kitettsége sokszorosára nőtt a kibertérből érkező támadásokkal szemben. Napjainkban az imént említett célszoftverek, vagyis egy számítógépre telepített víruskereső és tűzfal kombinációja az alapvető biztonság szavatolásához is kevés lehet, ha emellett nem gondoskodunk adataink, kommunikációs csatornáink és okoseszközeink védelméről, nem használunk megfelelő hosszúságú és bonyolultságú jelszavakat, többlépcsős azonosítási módszereket, és nem ismerjük fel időben az emberi hiszékenységen, illetve megtévesztésen alapuló támadásokat (social engineering).

Az átlagos felhasználó jellemzően nincs tisztában azzal, hogy a kibertámadásokkal szembeni kitettsége mekkora mértéket ölt, és nem is lehet reális elvárás, hogy mindenki önmaga kiberbiztonsági szakembere legyen. Ugyanakkor a kiberbiztonsági tudatosság fejlesztésére és terjesztésére egyre jelentősebb igény mutatkozik, hiszen a kibertér sajátosságaiból fakadóan az egyén tájékozatlansága és felelőtlen felhasználói magatartása könnyedén megbéníthat egy egész szervezetet, de akár veszélyt jelenthet a nemzetbiztonságra is. A kibertérben nincsenek államhatárok, ahol ellenőrzést lehetne folytatni. Az ott zajló események gyakran a másodperc tört része alatt következnek be, miközben hatásuk évekig eltarthat, a folyamatok attribútumainak bizonyító erejű meghatározása pedig a legtöbb esetben rendkívül bonyolult, sokszor lehetetlen. Szintén eltér a hagyományos (offline) világunk

szabályszerűségeitől, hogy a kibertérben a nemzetállamok korántsem egyeduralkodók: itt a társadalom megannyi szereplője megtalálható, a multinacionális cégektől a szervezett bűnözői és aktivista csoportokon át egészen az egyéni felhasználóig. A kibertér említett jellemzői jól mutatják, hogy milyen sokszínű és bizonyos tekintetben mennyire eltérő a virtuális világ a hagyományoshoz képest.

A kibertér sajátosságait figyelembe véve a nemzetállamok a világon mindenütt próbálnak a hagyományos területekkel foglalkozó nemzetközi együttműködésekhez hasonló szövetségeket létrehozni a kibertér biztonságának szavatolása érdekében. Ezek az együttműködési kezdeményezések elsősorban az elmúlt évek kiberbiztonsági trendjeinek köszönhetők, amelyek rádöbbentették a kormányokat arra, hogy önállóan nem képesek megvalósítani a kibertér biztonságos használatának alapvető feltételeit. A kibertérhez kapcsolódó nemzetközi együttműködések legtöbbször a szabályozatlanság problémájára próbálnak megoldást találni, de egyre több a kiberbűnözés elleni, határokon átnyúló összefogás, illetve a szellemi tulajdon védelmében és a kibertérben folytatott kémkedés ellen létrehozott multinacionális kooperáció. Magyarország több nemzetközi kiberbiztonsági kezdeményezésben is érintett egyrészt az euroatlanti szövetségi rendszerhez kapcsolódó beágyazottsága, másfelől az önálló, illetve harmadik fél általi regionális kezdeményezések révén. Utóbbiak közül kiemelkedő a 2013 májusában Ausztria és Csehország kezdeményezésére létrehozott Közép-európai Kiberbiztonsági Platform (Central European Cyber Security Platform, CECSP), melynek hazánk mellett Lengyelország és Szlovákia is tagja.

Annak érdekében, hogy egy szervezet különböző szintjein megjelenő kiberbiztonsági probléma kapcsán ne csak az aktuális kihívást lássuk, és adott esetben az akut elhárításon, illetve „tűzoltáson" túl hosszabb távú megoldást lehessen kidolgozni, érdemes egy pillanatfelvételt készítenünk azokról a nemzetközi kiberbiztonsági trendekről, amelyekre az előző bekezdésben már utaltunk. A biztonságpolitikai megközelítés egyik alapja, hogy egy incidens vagy konfliktus kialakulása számos tényezőre vezethető vissza. Ezeknek feltérképezésében és azonosításában jelentős szerepe van a körülöttünk zajló lokális, regionális és globális folyamatoknak, melyeknek értékelése és figyelemmel követése elengedhetetlen ahhoz, hogy a szükséges helyen és időben megfelelően felkészültek lehessünk. Az offline világunk hagyományos incidenseihez vezető út elemzése, az események monitorozása, illetve újabbak előrejelzése olyan tevékenység, amely teljes mértékben alkalmazható a kibertérre vonatkozóan is, így a kiberbiztonsági problémák kezelhetőbbé válnak.

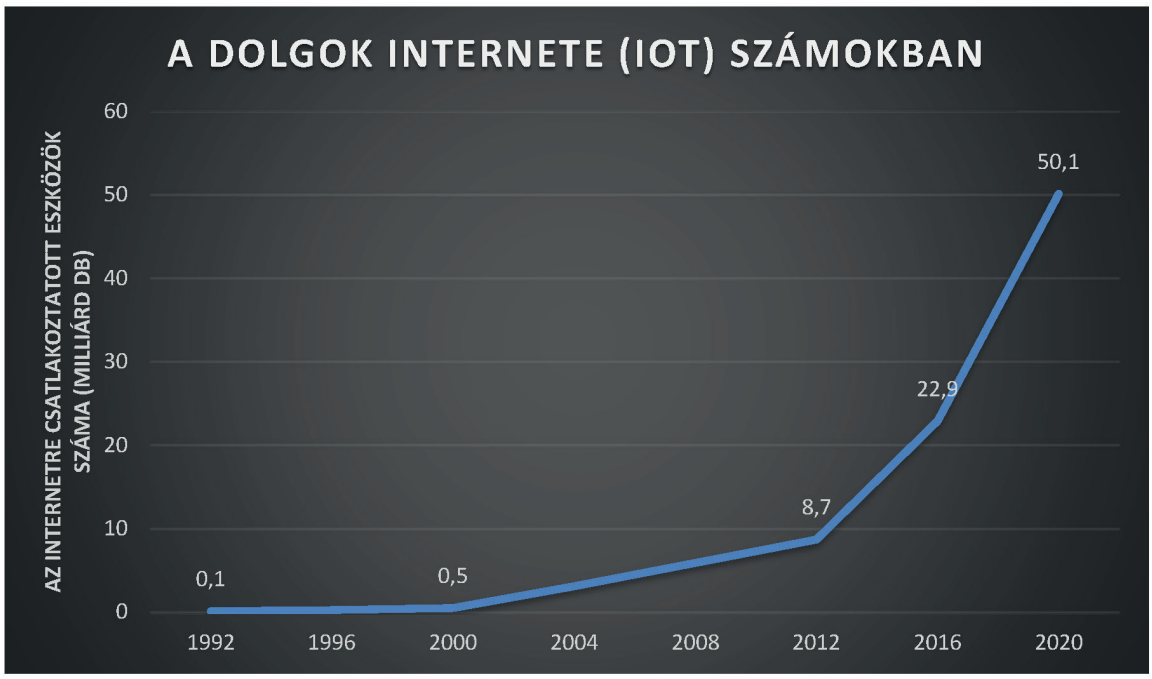
1.2. Biztonsági trendek a kibertérben

Amikor kiberbiztonsági kérdésekkel foglalkozunk, előbb vagy utóbb fontos szerepe lesz a kibertérben zajló folyamatoknak és trendeknek, illetve az ezeket számszerűsítő kimutatásoknak és statisztikai adatsoroknak. Például egy kiberbiztonsági incidens kapcsán az egyik elsőként felmerülő kérdés, hogy hány felhasználót vagy rendszert érint az adott eset. Annak érdekében, hogy tisztában legyünk az ember alkotta virtuális világ méretével, népességével és arányaival, ajánlott az aktuális trendeket áttekinteni. Számos forrás és adatsor található arra vonatkozóan, hogy hány ember él a világon, és használja manapság az internetet, ugyanakkor az egyes földrajzi és gazdasági régiók között jelentős eltérések mutatkoznak, több tekintetben is. Az egyik megbízható forrásnak számító Nemzetközi Távközlési Egyesület (International Telecommunication Union, a továbbiakban: ITU) 2016 júniusában kiadott adatai szerint a világ lakosságának több mint fele továbbra sem fér hozzá az internethez. Ugyan az ITU szerint 2016 végére 3,9 milliárd főre csökkent azoknak a száma, akik nem használják az internetet, regionális bontásban például Afrikában a lakosság 75%-a nem fér hozzá a világhálóhoz, miközben Európában ugyanez az arány csupán 21%. Az adatok sajátos bemutatása az ENSZ fenntartható fejlődési célkitűzéseihez köthető, ha azonban megfordítjuk a megközelítést, azonnal látható, hogy 47%-os lefedettség mellett, globális szinten majdnem minden második ember hozzáféréssel rendelkezik a világhálóhoz. Európában a háztartások 84%-a csatlakozik az internethez, miközben a széles sávú mobil előfizetések aránya meghaladja a 76%-ot (*ICT Facts and Figures 2016*.).

A 738 millió fős európai lakosságra (UN ESA, 2015) vetítve ez több mint félmilliárd felhasználót jelent csak az öreg kontinensen. Tovább szűkítve a vizsgálati kört, Magyarországon a rendszeres internethasználók aránya eléri a 72%-ot (*Rendszeres internethasználók aránya (2005–2016)*), ami több mint 7 millió felhasználót jelent hazánkban.

Más megközelítésben érdemes elgondolkodni azon, hogy mi történik az interneten, ha egyetlen szűk perc keresztmetszetét próbáljuk megvizsgálni. Egy 2016 nyarán megjelent felmérés szerint gigantikus méreteket ölt a különböző online tartalmak generálása. A kutatási eredményeket publikáló jelentés „tartalomsokknak" nevezi a jelenséget, aminek következtében a 2013-ban egy perc leforgása alatt elküldött e-mailek száma 182,9 millióról 2015-re 205,6 millióra nőtt. De hasonló adatokat mutat a legnépszerűbb internetes keresőmotor (Google) használata is: itt a 2013-as egy perc alatt indított 2,6 millió keresés 2015-re elérte a 3,1 milliót, míg a világelső közösségi oldalon (Facebook) közzétett posztok száma 2,5 millióról 3,3 millióra nőtt. Ennél is jelentősebb a változás a legnépszerűbb közösségi videomegosztó (YouTube) oldal esetében, ahol 2013-ban egy perc alatt még csak 100 órányi tartalmat töltöttek fel a felhasználók, 2015-ben viszont már 400 órányit. Szignifikáns a különbség az egyik népszerű azonnali üzenetküldő alkalmazás (WhatsApp) esetében is, amelynek segítségével a felhasználók 2013-ban még 11,8 millió üzenetet küldtek egy perc leforgása alatt, 2015-ben viszont már 44,4 millió üzenetet továbbított ugyanez az alkalmazás percenként (Hubspot, 2016). Az említett adatok azt mutatják, hogy jelentős és folyamatos növekedés mutatkozik mind a felhasználók számában, mind pedig a felhasználás mértékében. A kiberbiztonság jelentőségének megértéséhez további folyamatokat is feltétlenül figyelembe kell venni, melyek közül kettőt fontos kiemelni.

Korábban már szóba került, hogy a mindennapi életünk során egyre több szálon kapcsolódunk a virtuális világhoz. Míg korábban elsősorban az asztali vagy hordozható számítógépünk segítségével kommunikációra használtuk a kiberteret, később pedig pénzügyi tranzakciók lebonyolítására vagy multimédiás tartalmak fogyasztására, ma már egyre több eszközünk kapcsolódik a kibertérhez, amelyek a legkülönbözőbb funkciókon keresztül képesek digitalizálni mindennapjainkat. Gondoljunk a manapság oly divatos okoseszközökre (telefonok, televíziók, karórák stb.), melyek mindegyike egy-egy újabb szálon kapcsol bennünket a kibertérhez. Az okos eszközök által dominált virtuális világ angol elnevezése az Internet of Things (IoT), vagyis *a dolgok internete,* és ez jóval túlmutat a ma elterjedt okoseszközök képességein és lehetőségein. A dolgok internete tulajdonképpen nem más, mint hálózatba kapcsolt eszközök, járművek, épületek és egyéb ember alkotta tárgyak, amelyek a beépített elektronikának, szoftvereknek és szenzoroknak köszönhetően képesek egymással kommunikálni a hálózati kapcsolataikon keresztül. Ezek az eszközök távoli eléréssel, a hálózaton keresztül érzékelhetők és irányíthatók, aminek köszönhetően egyre inkább elmosódik a határ a fizikai és a virtuális világ között. Az ITU 2012-ben kiadott ajánlása értelmében az IoT nem más, mint az információs társadalom infrastruktúrája (*Overview of the Internet of Things, 2012*.). Az előrejelzések alapján az IoT térnyerése következtében robbanásszerűen megnövekszik az internethez csatlakoztatott eszközök száma az elkövetkező néhány évben. Már most is közel 23 milliárd eszköz csatlakozik az internethez globális szinten, de ez a szám 2020-ra elérheti, sőt nagy valószínűséggel meg is haladja majd az 50 milliárdot! Ez azt jelenti, hogy a világ 7,4 milliárd lakójára vetítve már ma is minden földlakó három különböző eszközzel éri el az internetet.



1. ábra

Az internetre csatlakozó eszközök száma 2012 után kezdett igazán dinamikus növekedésbe, aminek eredményeként 2020-ra több mint 50 milliárd eszközzel csatlakozunk a virtuális világhoz.

Forrás: A CompTIA Projecting *The 'Things' Behind the Internet of Things* grafikonja alapján szerkesztette a szerző. Az eredeti grafikon elérhető: http://blogs-images.forbes.com/gilpress/files/2016/08/Slide2.jpg?width=960 (a letöltés ideje: 2016. november 4.)

A IoT térhódítása több szempontból is megállíthatatlannak tűnik. Az internetre csatlakoztatott eszközök száma már 2008-ban meghaladta a Föld népességének számát (Evans, 2011), 2017-ben pedig az IoT-eszközök piaca nagyobb lesz, mint az asztali számítógépek, tabletek és telefonok piaca együtt (The Internet of Everything 2014). Ez számokban kifejezve azt jelenti, hogy a 2013-as 1,9 billió dolláros szintről 2020-ra az IoT-piac 7,1 billió dollárra nő (IoT: Hottest technology to watch out for in 2015. *The Economic Times,* 2015).

Hamarosan olyan hétköznapi használati tárgyaink és eszközeink is kapcsolatban lesznek a kibertérrel, mint az autónk, a háztartási eszközeink (hűtő, mosógép, sütő, kávéfőző stb.) vagy akár az otthonunk teljes gépészeti, elektromos és egyéb rendszerei. A trendekből kirajzolódó folyamatnak azonban van egy árnyoldala is, amivel a kibertérben komoly károkat okozhatnak a rossz szándékú felhasználók. Jó példa erre a világ egyik legjelentősebb kiberbiztonsági konferenciája, a DefCon, ahol 2016-ban 21 gyártó 23 eszközében összesen 47 sérülékenységet mutattak be a résztvevők (Mészáros, 2016). Ugyanakkor a már jelenleg is kiterjedt támadási felület nagyságát jól szemlélteti egy 2015-ben megjelent tanulmány, amely azt vizsgálta, hogy milyen szintű Magyarország kiberbiztonsági kitettsége az internethez csatlakozó ipari folyamatirányító rendszereknél, amelyek jellemzően erőművek vezérléséért, a közüzemi szolgáltatások működésért vagy éppen különféle gyártósorok üzemeltetéséért felelősek. A tanulmányban bemutatott, 4 és fél óra alatt elvégzett mérés eredményei szerint 6100 olyan támadási pont volt található a kibertérben, amin keresztül a hazai szolgáltatások és infrastruktúrák működése megzavarható vagy leállítható lett volna, és milliós nagyságrendűre becsülhető azoknak a sérülékenységeknek a száma, amelyek kritikus infrastruktúrákat irányító rendszerekben találhatók (Berzsenyi–Ványi, 2015).

A bemutatott példák és adatok a kiberbiztonsági trendeket csak nagy vonalakban ábrázolják, azonban a bevezetőben leírt dinamikus növekedést, a kibertér hódítását és a kihívások párhuzamos növekedését jól alátámasztják. Az egyre nagyobb kitettség következtében új szegmensek jönnek létre a különböző iparágakon belül, amelyre jó példa az egyelőre főként nagyvállalati környezetben terjedő

kiberbiztosítás. Az egyik legújabb biztosítási piac lényege, hogy a vállalatok az egyre jobban elterjedő digitalizált folyamatok következtében olyan veszélyekkel és veszteségekkel szemben is szeretnének fedezetet, amelyek a kibertérből érkeznek. A kibertámadások személyre, iparágra, nemzetre való tekintet nélkül mindenkit fenyegetnek, így az összes kapcsolódó kihívás áttekintése jelen esetben a teljes tankönyv határain is nagyságrendekkel túlmutatna. Ezért a rendelkezésre álló kereteket a legfontosabb és leginkább aktuális, nemzetközi biztonságpolitikai vonatkozású kiberbiztonsági kihívások bemutatására használjuk fel.

1.3. A lokális folyamatokat érintő kiberbiztonsági kihívások

Sokakban valószínűleg már az alcím olvasása közben felmerül a kérdés, hogyan kerülhetnek lokális folyamatok egy alapvetően nemzetközi biztonságpolitikai kihívásokat tárgyaló fejezetbe. A kérdés jogos, amire egyszerű a felelet: a választások külföldi befolyásolása. A fejlett nemzetek számára – választási rendszertől függetlenül – a demokratikus választás és annak külső behatás nélküli lebonyolítása az államiság egyik alapját jelenti. De az államok belügyeibe történő külső beavatkozás nemcsak a demokratikus elvek mentén működő államok problémája: bármely állam számára a XXI. század első felének egyik legnagyobb kihívása, hogy a belső politikai folyamatait miként óvja meg a külső befolyásolástól.

A befolyásolás nem újkeletű jelenség a nemzetállamok között, az régóta működik szabályozott és szabályozatlan keretek között egyaránt. Ami az újdonság, az a kibertér szerepének jelentős megnövekedése. Az említett befolyásolásnak egy új dimenzióját láthatjuk napjainkban, az Amerikai Egyesült Államokban lezajlott 2016-os választásokat követően, illetve a 2017-es francia választások közben. Nagy valószínűséggel az elkövetkező évek során nem is lesz olyan választás, amit ne érintene valamilyen szinten a kibertérből érkező kihívás. Legyen szó a választási adatok megváltoztatásáról, a választási kampányba történő beavatkozásról vagy a szemben álló felek politikai ellehetetlenítéséről, a legtöbb állam egyelőre csak keresi azokat a megoldásokat, amiknek a segítségével a kibertérből érkező kihívásokat minimalizálni lehetne a választásokkal összefüggésben.

Az Amerikai Egyesült Államokban lezajlott legutóbbi választások során a kibertérnek, illetve a kibertérből érkező fenyegetéseknek igen nagy jelentőséget tulajdonítottak az egész világon. Mivel az USA továbbra is a világ első számú katonai hatalma, szerte a világon nagy figyelemmel kísérték a választási kampányt és az azt megelőző eseményeket. Bár a mai napig több „kibertámadásként" emlegetett esemény bizonyítatlan, illetve a részletek ismeretlenek, a befolyásolásra utaló jelek mértéke akkora, hogy nem lehet őket figyelmen kívül hagyni. 2016. június közepén kerültek a nyilvánosság elé az első olyan információk, amelyek arra utaltak, hogy a választásokat is érintő kiberbiztonsági incidens történt a Demokrata Nemzeti Bizottságnál (Democratic National Committee, a továbbiakban: DNC). Rövid időn belül a feltételezett tetteseket is bejelentették, ami szerint az elkövetők az orosz kormányhoz köthető *Fancy Bear,* illetve *Cozy Bear* néven ismert hackercsoportok. Néhány nappal később a Wikileaks portál mintegy 20 000, DNC-szerverekről származó e-mailt hozott nyilvánosságra, amire válaszként az Amerikai Egyesült Államok Szövetségi Nyomozó Irodája (Federal Bureau of Investigation, a továbbiakban: FBI) nyomozást indított.

Néhány héttel később, 2016. augusztus közepén a DNC vezetőinek adatai szivárogtak ki, majd a nyár hátralevő része kölcsönös nyilatkozatháborúba fulladt az orosz fél, illetve a két amerikai elnökjelölt és stábjaik között. Már javában futott az amerikai elnökválasztási kampány, amikor újabb 58 000 üzenet került nyilvánosságra a Wikileaks jóvoltából, egyenesen a demokrata jelölt kampányfőnökétől. 2016 őszére az amerikai hatóságok egybehangzóan Oroszországot nevezik meg a választások körül kialakult helyzet okozójaként, azonban a motivációban bizonytalanság mutatkozik. Az elindított vizsgálatoknak köszönhetően kiderült, hogy a DNC sorozatos hibákat követett el, és nem az elvárható módon reagált a kiberbiztonsági incidensekre, ami hozzájárulhatott a támadások sikeréhez. A választások körül kialakult botrány következtében végül az USA szankciókat vezetett be Oroszországgal szemben, és 35 orosz diplomatát 72 órás határidővel kiutasítottak az országból. A titkosszolgálatok

vizsgálati eredményei alapján a választásokat közvetlenül nem befolyásolták, a szavazógépek és a szavazások lebonyolításához használt számítógépek nem kompromittálódtak.

A 2017-es franciaországi választások során is történt olyan esemény, amely a választások kibertámadásokkal szembeni kitettségére hívja fel a figyelmet. 2017. április 25-én a Trend Micro nevű cég elemzői bejelentették: bizonyítékokkal rendelkeznek arra vonatkozóan, hogy a francia elnökválasztási kampány egyik jelöltjét és stábját támadja a *Fancy Bear* (APT28) néven ismert hackercsoport. A támadás kapcsán kiadott jelentés szerint a kampánystáb tagjai célzott adathalász e-maileket kaptak, amelyek a politikai mozgalom honlapja helyett fertőző oldalakra irányították a felhasználókat. A támadók arra is figyeltek, hogy a támadáshoz használt weboldalakhoz az eredeti oldalak címeihez hasonló neveket használjanak. Ezt követően május 6-án több ezer e-mail vált nyilvánosan elérhetővé az En Marche! mozgalom belső levelezőrendszeréből. A mozgalom közleménye szerint a kampánystáb egy kiterjedt és összehangolt hackertámadás áldozatává vált, aminek következtében számos belső információ került be a közösségi médiába. Az áldozatok külön kiemelték, hogy több dokumentum is úgy terjed a világhálón, hogy az eredeti szövegrészeket fiktív elemekkel keverték össze, így alkalmassá téve azokat a megtévesztésre és a súlyos dezinformáció terjesztésére.

A választások befolyásolására irányuló kísérletek minden jel szerint a következő évek velejárói lesznek, ezért fontos lenne, hogy a problémával nemzetközi szinten foglalkozzanak az érintett felek. 2017-ben tartanak még egy európai uniós viszonylatban jelentősnek számító választást Németországban, 2018-ban pedig Magyarországon is választások lesznek. Németország jelentős erőkkel készül a választások kibertámadásokkal szembeni megvédésére, aminek egyik publikus jele, hogy a német Szövetségi Alkotmányvédelmi Hivatal (Bundesamt für Verfassungsschutz, a továbbiakban: BfV) vezetője nyíltan beszélt egy konferencián a befolyásolásról és az egyre agresszívabbá váló kiberkémkedési tevékenységről. A német hatóságok ellehetetlenítik, szükség esetén működésképtelenné teszik azokat a szervereket, amelyeknek az üzemeltetői, illetve tulajdonosai nem képesek garantálni, hogy azokat ne használják fel kibertámadásokhoz (Rettmann, 2017). Amennyiben a német választásokat valóban kibertámadás éri valamilyen formában, és a német hatóságok a bejelentésnek megfelelően járnak el, ez lehet az első olyan nyilvános eset, ahol egy állam támadó képességeket vet be, és visszatámad (hackback) a kibertérben.

1.4. A regionális folyamatokat érintő kiberbiztonsági kihívások

Általánosságban elmondható: egyre inkább jellemző az, hogy a konfliktusok által sújtott régiókban az egymással szemben álló felek a kibertérben is aktív tevékenységet folytatnak. A biztonságpolitikai elemzők az elsők között szokták említeni a 2008-ban Oroszország és Grúzia között lezajlott fegyveres összecsapást, amelynek nemcsak előkészítése során, de a katonai műveletek ideje alatt és azt követően is jelentős szerep jutott a kibertérben folytatott műveleteknek. A fegyveres harcokhoz képest hetekkel korábban megindultak az elosztott szolgáltatás megtagadásával (Distributed Denial of Service, továbbiakban DDoS) járó támadások: számos honlap és szerver vált hosszabb-rövidebb időre elérhetetlenné, erősen akadozott a kommunikáció az érintett területeken. A támadók gyakorlatilag információs blokád alá vették Grúziát. 2008-ban a grúz kormány a támadások elkövetésével az oroszokat vádolta meg, azonban az orosz kormány szóvivője a vádakat azzal hárította, hogy lehetnek olyan hazafias magánszemélyek Oroszországban, akik így nyilvánítják ki véleményüket. A Torontói Egyetem egyik szakértője az eseményeket követően azt nyilatkozta, hogy „méretét és a nemzetközi dimenziókat figyelembe véve mérföldkő a támadás” (Hart, 2008). Korábbról valóban nem tudunk olyan példát felhozni, amikor egy reguláris erőkkel vívott küzdelmet az előkészítéstől a lezárást követő időszakig ilyen volumenű kibertevékenység kísért.

Egy biztosan látszott már a 2008-as eseményeket követően is: a kibertámadások olcsón és egyszerűen kivitelezhetők, hiszen néhány száz számítógép és pár képzett hacker elegendő ahhoz, hogy egy országot blokád alá vonjanak a kibertérben. Szintén jól kirajzolódott, hogy a támadók célja nem

pusztán a kommunkáció bénítása volt, hanem a kommunikáció *kontrollja* is, vagyis ebben az esetben az orosz támadásokat előkészítő és segítő propaganda terjesztése. Bár jó esély van arra, hogy soha nem derül ki teljes bizonyossággal a támadók kiléte, a konfliktusok legalapvetőbb szabálya, hogy mind a támadó, mind a védő fél egyértelműen azonosítsa a másik felet. A fegyveres konfliktusokat szabályozó hadijog mindezt részletesen kifejti, azonban olyan időket élünk, amikor a felek azonosítása nemcsak a fizikai világban válik egyre nehézkesebbé a gerilla hadviselés, illetve a terrorista módszerek elterjedése miatt, de a kibertér sajátosságaiból fakadóan szinte lehetetlen meghatározni, hogy egy-egy kibertámadás mögött egy másik nemzet, egy politikai csoportosulás vagy esetleg egy bűnszervezet áll. 2008 óta ez a terület szinte érintetlen maradt, és nem igazán sikerült sem technikai, sem szabályozói oldalról olyan megoldásokat kidolgozni, amelyek a kibertámadások elkövetőinek felelősségre vonását és a bizonyítást elősegítené.

De nem feltétlenül kell egy konfliktusnak a fegyveres összecsapásokig eszkalálódniuk ahhoz, hogy valamelyik fél kibertámadáshoz folyamodjon. Kiváló példa erre a bő egy évvel korábban, 2007 tavaszán történt észtországi kiberkonfliktus, amelynek kirobbantásával szintén Oroszországot vádolták meg. A kibertérben végrehajtott műveleteket 2007. április 27-én az észt fővárosban, Tallinnban kitört zavargások előzték meg, melyek egy szovjet hősi emlékmű elköltöztetése miatt alakultak ki. Ebben az esetben is DDoS-támadások játszották a főszerepet, melyek néhány nappal a tüntetéseket követően kezdődtek, és alapvetően észt kormányzati hivatalokat, minisztériumokat és a parlamentet vették célba. Ugyanakkor számos pénzügyi intézmény, telekommunikációs vállalat és médiacég szerverei is megbénultak. Akkoriban a célpontok kiválasztása, a támadások előkészítettsége és precíz végrehajtása, valamint volumene egyaránt arra utalt, hogy átlagos hackereknél komolyabb erők állnak a háttérben, vagyis egy nemzetállam által támogatott támadásról volt szó, ami a tallinni események nyomán leginkább az oroszoknak állhatott érdekében.

Bár a világon a sajtó mindenütt úgy tálalta az események következményeit, mintha azok katasztrofálisak lennének az észt társadalomra nézve, ha Tallinnban járunk, és egy kicsit utána kérdezünk, hamar kiderül, hogy az átlagemberek életében korántsem okozott akkora fennakadást a támadássorozat, mint azt kívülállóként gondolnánk. A nagyjából két hét alatt 128 túlterheléses támadást regisztráltak. Ezek között volt, amelyik csak néhány óráig, és volt, amelyik napokig tartott, továbbá számtalan oldalt feltörtek és módosítottak, jellemzően valamilyen oroszbarát tartalommal. Mivel Észtország ekkor már 4 éve a NATO tagja volt, viszonylag gyorsan felmerült a kérdés, hogy katonai akciónak minősíthető-e a kibertérben végrehajtott támadás, és ilyen esetben is érvénybe léptethető-e a NATO 5. cikkely szerinti segítségnyújtás a többi tagállam részéről, de akkoriban nem mutatkozott egyetértés ebben a kérdésben, így a NATO-szakértők végül nem minősítették katonai támadásnak az esetet.

Nem kérdéses azonban a jelenlegi ukrán konfliktus kapcsán, hogy katonai műveletekről van szó. Az orosz fél érintettsége itt is erőteljes, azonban Oroszország hivatalosan nem ismeri el, hogy katonai hírszerzőkön kívül komolyabb erőt alkalmazna egy másik állam területén. Bár széles körben ismertté váltak a 2015 végén az ukrán energetikai rendszer ellen elkövetett kibertámadások, az Ukrajnában zajló fegyveres konfliktusról kevésbé ismert, hogy a grúz esethez hasonlóan aktív kiberműveletek zajlanak a háttérben. A 2014-es ukrán választásokig nyúlnak vissza az ismét Oroszország számlájára írt kibertámadások, amelyek elsőként a választási bizottságot célozták annak érdekében, hogy az eredményeket befolyásolni lehessen. Az akkori hírek szerint a támadás olyan sikeres volt, hogy még a biztonsági mentéseket is sikerült tönkre tenni. Végül a szavazást segítő rendszerek működtek, de a választási bizottság honlapján a támadóknak sikerült meghamisított eredményeket elhelyezniük, amit azután a média is átvett. Mindez persze a választás eredményét végül nem befolyásolta, azonban a kormányzat és a közigazgatási szervek integritását, valamint a beléjük vetett bizalmat jelentősen rombolta. A választások támadását követően az ukrán bankrendszert, a vasúthálózatot és több bányaipari céget is támadás ért. Az ukrán vezetés mindvégig Oroszországot tette felelőssé a kibertámadásokért, az oroszok pedig szokás szerint tagadták a vádakat. Felmerült az is, hogy Oroszország a katonai műveletek során olyan hatékonyan alkalmazta kibertámadási képességeit, hogy az ukrán hadsereg tüzérségének jelentős veszteségei is ennek köszönhetők. A bizonyítás itt is elmaradt, ráadásul a szakértők

között sincs egyetértés abban, hogy az ukránok súlyos tüzérségi veszteségei és az oroszok által a kibertérben folytatott műveletek között valóban összefüggés mutatható ki. Egyes elemzők szerint az Ukrajna ellen bevetett kiberfegyvereket ugyanaz az orosz állami támogatással működő és az orosz katonai titkosszolgálathoz kötődő *Fancy Bear* (APT28) néven ismert csoport alkalmazza, amelynek az Amerikai Egyesült Államokban a DNC megtámadását is tulajdonítják. Pró és kontra számos érvvel találkozhatunk, azonban a támadó kilététől függetlenül is kijelenthető, hogy az ukrán konfliktusban ismét jelentős szerephez jutott a kibertér, illetve az ott folytatott műveletek.

Időközben 2016 nyarán a NATO elismerte a kiberteret a háború, illetve a hadviselés ötödik dimenziójaként, ami jelentős előrelépés több tekintetben is. Egyfelől a szövetség keretein belül ezentúl a kiberképességek fejlesztésére a többi dimenzióhoz (szárazföld, tenger, levegő, világűr) hasonlóan lehet célzott fejlesztéseket kialakítani és forrásokat allokálni, másfelől a kibertérből érkező támadások katonai akcióként történő elismerése egyértelműbb. Ha a kibertérből érkező támadás akár emberéletben, akár gazdasági károkban felér egy fizikai támadással, akkor előfordulhat, hogy arra válasz is érkezik, és adott esetben nemcsak a kibertérben, hanem fizikai csapás formájában. Bár nem a NATO hajtotta végre, de a kibertérben zajló folyamatokra adott fizikai válaszokra jó példa az Iszlám Állam első számú hackereinek az USA által történő felkutatása és likvidálása drónok segítségével.

A biztonságpolitikai elemzők számára kirajzolódó trendek azt mutatják, hogy a folyamatos kapacitás- és képességbővülés a kibertérben nagyon élénkké vált az utóbbi években. Sok esetben hosszú évek fejlesztései és ráfordításai kezdenek láthatóvá válni, és egyre több azoknak az államoknak a száma, amelyek a kibervédelmi képességek mellett támadó képességeket is fejlesztenek. Ilyen tekintetben jelenleg az első 5 ország között találjuk Oroszországot, Kínát, Iránt, Észak-Koreát és az USA-t, de egyre meghatározóbb képességekre tesz szert Izrael, Pakisztán, illetve India is. A folyamatok egyértelműen azt mutatják, hogy egyfajta „kiberfegyverkezési verseny" van folyamatban, ami természetesen nem az utóbbi néhány év eredménye. Pusztán arról van szó, hogy a felhalmozott képességek nyílt bevetése és alkalmazása nyomán ezek a folyamatok többé már nem a felszín alatt zajlanak.

A kiberbiztonság különböző szegmenseit tárgyalva észre kell vennünk a kapcsolódási pontokat az adatvédelem területéhez, ahol szintén komoly regionális folyamatok zajlanak, elsősorban az Európai Uniónak (a továbbiakban: EU) köszönhetően. Az EU-ban már eddig is számos rendelkezés biztosította a személyes adatok védelmét, de 2018. május 25-től új szintre emelkedik az adatvédelem az EU területén. Az új adatvédelmi szabályozás megalkotásának egyik oka az volt, hogy az érvényben lévő szabályozás egyre kevésbé volt alkalmazható a rohamos léptekben fejlődő információs társadalomban zajló folyamatokra. Az új szabályozás kialakításának másik oka az volt, hogy az EU döntéshozói meg kívánták erősíteni a magánszemélyek online szolgáltatásokba vetett bizalmát, illetve az online környezettel jobban harmonizáló, korszerű adatvédelmi jogszabályt szerettek volna létrehozni.

Az EU Általános Adatvédelmi Rendelete (General Data Protection Regulation, a továbbiakban: GDPR) minden tagállamban, így hazánkban is adatvédelmi reformmal jár együtt, és minden személyes adatot kezelő szervezetre kiterjed. Többek között a GDPR-nek köszönhetően módosul hazánkban az adatvédelmi törvény, a Kiberbiztonsági Stratégia, valamint az információbiztonsági törvény és azok a vonatkozó részletszabályok, amelyek nincsenek összhangban az EU-rendelettel. Ennek szövege szerint a hatálybalépést követően minden ügyfél élhet az adatok hordozhatóságához és a felejtéshez fűződő jogával, ami azt jelenti, hogy egyfelől kérhetik szolgáltatójukat, hogy adataikat adja át másik szolgáltatónak, másfelől jogosultak a személyes adatok indokolatlan késlekedés nélküli törlését kérni. További újdonság az úgynevezett profilalkotás tiltásának joga, továbbá 2018-tól biztosítani kell az ügyfél számára a betekintés jogát. A rendelet egyik fontos – és az elmúlt évek tömeges felhasználói adatlopásait figyelembe véve (gondoljunk csak az OPM vagy a Yahoo botrányára) kiberbiztonsági szempontból is jelentős – passzusa, hogy a személyes adatot álnéven kell tárolni, pont azért, hogy a felhasználói adatokat tartalmazó adatbázis kompromittálódása esetén a személyiségi jogok ne sérülhessenek. A rendelet megalkotói megelőző intézkedéseket is előírnak, így minden olyan szervezet köteles adatvédelmi hatástanulmányt készíteni, amely jelentős mennyiségű személyes adatot kezel, illetve amelynél az érintettek adatai veszélyben lehetnek. Lényeges pont, hogy 2018-tól a szervezetek

kötelesek az adatvédelmet, illetve a felmerülő költségeket beépíteni az üzleti folyamataikba és a rendszerek tervezésébe egyaránt. Szintén az elmúlt évek milliós és milliárdos nagyságrendű adatvesztéseinek egyik sajátosságát kívánják a rendelet megalkotói felszámolni azzal, hogy egy incidens esetén arról legkésőbb 72 órán belül értesíteni kell a nemzeti adatvédelmi hatóságokat. Az érintettekre nézve jelentős kockázat esetén azokat is kötelező tájékoztatni, akiknek az adatait az incidens érinti. Az EU súlyos szankciókat helyezett kilátásba bírság formájában, amely egységes mértékű lesz mindenütt, és a legsúlyosabb incidensek esetén elérheti a társaság árbevételének 4 százalékát, amit 20 millió euróban maximalizáltak.

Összességében a GDPR az egyik legfontosabb eleme az Európai Unió kiberbiztonság terén tett erőfeszítéseinek, hiszen olyan egységes, minden tagállamra kiterjedő, a személyes adatokat védő rendelet, amely egyértelműen a felhasználók védelmében született, és erős kényszerítő hatást fejt ki az adatkezelőkre az általuk tárolt személyes adatok biztonságának növelése érdekében. A korábban említett tömeges adatlopások nagy valószínűséggel ettől még nem fognak megszűnni, azonban jó esély van arra, hogy egyre kevesebb, a felhasználókra nézve komoly kockázatot jelentő incidens történik az EU területén. Az EU rendeletbe foglalt adatvédelmi törekvései regionális szinten hatékony nemzetközi választ jelenthetnek az aktuális kiberbiztonsági kihívásokra, de csak akkor, ha az implementáció sikeresnek bizonyul, és azon kis- és középvállalkozások számára is elfogadható mértékű lesz a rendeletből fakadó plusz költségek mértéke, amelyek jelenleg a leginkább kitettek a kibertámadásokkal szemben.

1.5. A globális folyamatokat érintő kiberbiztonsági kihívások

Globális szinten egyre több a kibertámadás, amelyek egyre szofisztikáltabbak is, ugyanakkor azoknak a támadásoknak is meredeken emelkedik a száma, amelyekhez nem szükséges különösebb technikai tudás. A tudástranszfer következtében ma már minimális beruházással és informatikai tudással is lehet valakiből támadó. A kiberbiztonsági fenyegetések és kihívások kapcsán fontos forrásnak tekinthetők az ezen a területen működő, jelentős ügyfélkörrel rendelkező biztonsági cégek, nagy tekintélyű kutatóközpontok és egyéb kiberbiztonsági szakembereket tömörítő szakmai szervezetek, amelyek időszakos felmérésekkel, beszámolókkal, éves jelentésekkel és rendszeres adatmegosztással segítik egymás és a kiberbiztonsági közösség munkáját.

A rendelkezésre álló legfrissebb adatok alapján csökkent a különböző rosszindulatú szoftverek által megfertőzött számítógépek átlagos helyreállítási költsége, ugyanakkor nőtt a kiberbűnözők által okozott kár. A Kaspersky Cybersecurity Index alapján 2016-ban a második fél évben a felmérésben részt vevők 74%-a vélte úgy, hogy őt nem érinthetik az online fenyegetések, 39%-uk egyáltalán nem használt védelmi megoldást, 29% volt azok aránya, akik valamilyen kárt szenvedtek kibertámadás következtében. A korábbi 2016-os index ugyanebben a sorrendben 79, 40, 29%-os arányt mutatott, ami azt jelenti, hogy az első félévben több ember gondolta úgy, hogy nem eshet kibertámadás áldozatául és maradt védtelen. Szakértők szerint mindez arra utal, hogy bár nem túl gyorsan, de pozitívan változik az emberek hozzáállása az internetes biztonsághoz, és még ha lassan is, de folyamatosan nő azok száma, akik aggódnak a kibertérből érkező fenyegetések miatt, és tudatosan szeretnék megvédeni magukat a kibertámadásoktól. A Kaspersky felmérése alapján 2016 második félévében 22%-ról 20%-ra csökkent azoknak a felhasználóknak az aránya, akik valamilyen kártékony programmal találkoztak. Nőtt azonban azoknak a száma, akik egyéb, más típusú fenyegetések áldozataivá váltak, például zsarolóprogramok, adathalászat, adatlopás és adatszivárgás károsultjai lettek.

A Symantec éves jelentése alapján 2016-ban több egyedülálló támadásra is sor került. Volt példa több millió dollár eltulajdonításával járó virtuális csalásra, az USA választási folyamatába történő beavatkozásra és nem szabad megfeledkeznünk az eddigi egyik legnagyobb DDoS-támadásról sem, amit IoT-eszközökből alkotott gigantikus botnet segítségével hajtottak végre az elkövetők. Miközben a kibertámadások korábban nem látott mértékben zavarták meg a rendszerek működését, a támadók egyre gyakrabban használnak egyszerű eszközöket és taktikákat annak érdekében, hogy minél

nagyobb hatást válthassanak ki. A 0. napi sérülékenységekkel és a szofisztikált malware-ekkel a támadók egyre inkább takarékoskodnak, és gyakran támaszkodnak a célzott adathalászatra vagy más egyéb, nemegyszer legitim eszköz nem rendeltetésszerű használatára. 2016-ban ötéves csúcsot döntött a malware-t tartalmazó e-mailek aránya: 131 elküldött e-mailből egy biztosan tartalmazott kártékony elemet. A zsarolóvírusok továbbra is töretlenül szedik áldozataikat, a Symantec mérései alapján 2016-ban 36%-kal nőtt a zsarolóvírusos fertőzések száma, és az átlagos 300 dollár körüli váltságdíj több mint háromszorosára, 1077 dollárra nőtt. Korábban viszonylag ritka volt azoknak a kártevőknek a megjelenése, amelyek kifejezetten destruktív céllal működnek, azonban 2016 ebben a tekintetben is negatív tendenciát mutat. Két, egymástól független esetben is kimutatható volt a szabotázs szándéka kibertámadások során. Az egyik esetben az ukrán energiaellátó rendszereket támadták meg az év elején és az év végén is a BlackEnergy névre keresztelt kártékony szoftverrel, míg Szaúd-Arábiában a Shamoon tűnt fel újra különböző ipari és közigazgatási rendszerekben.

A globális kiberbiztonsági fenyegetések és kihívások további részletezése szükségtelen, hiszen a változás rendkívül dinamikus így érdemes a fenti adatokat is minden esetben a legfrissebb, rendelkezésre álló adatokkal behelyettesíteni. Ugyanakkor a bemutatott információkból is kirajzolódik, hogy a legtöbb kiberbiztonsági kihívás vagy az érintett felhasználók száma, vagy az okozott kár nagysága, esetleg a megtámadott rendszer jellege miatt nemzeti és nemzetközi szinten is jelentőséggel bír. Egy a kibertérben jelen levő állam ma már nem engedheti meg magának, hogy ne foglalkozzon a kiberbiztonsággal, és ne allokáljon forrásokat a biztonság szavatolására. Több kimutatás is azt bizonyítja, hogy a kiberbiztonságra költött összegek világszerte növekednek, szektoroktól függetlenül, azonban a károk is egyre nagyobbak.

Az International Data Corporation (IDC) 2020-ra szóló előrejelzése alapján a világ több mint 100 milliárd dollárt költ kiberbiztonsági szolgáltatásokra, szoftverekre és hardverekre. Az előrejelzés alapján ennek az összegnek közel a harmadát, mintegy 31 milliárd dollárt az USA fogja elkölteni különböző kiberbiztonsági eszközökre és szolgáltatásokra, míg a második helyen Nyugat-Európa áll 19 milliárd dolláros becsült költésével. Összességében a 2016-os évhez képest 38%-os a növekedés a kiberbiztonsági kiadások terén, de az nem derül ki, hogy ez milyen arányban oszlik el a 2020-ig hátralevő időszakban. Ehhez képest a kiberbűnözők számlájára írható kár nagysága már 2015-ben is elérte a 3 billió dollárt világszerte. Az érdekes az, hogy a 2016-os Cybercrime Report (Morgan, 2016) előrejelzése alapján 2021-re a kiberbűnözésből fakadó károk nagysága világszinten megduplázódik, és eléri a 6 billió dollárt. Ez magában foglalja a sérült és megsemmisült adatokat, az ellopott pénzt, a termelés kiesését, a szellemi termékek eltulajdonítását, a személyes és pénzügyi adatok ellopását, a sikkasztást, a csalást, a törvényszéki nyomozást és helyreállítást, valamint a reputációban keletkezett károkat.

Az IDC adataihoz képest a 2016-os Cybercrime Report nagyságrendbeli különbséget mutat a kiberbiztonsági termékekre és szolgáltatásokra vonatkozó kiadásoknál, mivel azt több mint tízszeresére becsüli! Bárhogy is történjen, a következő néhány évben továbbra is folyamatos és dinamikus növekedés várható a kiberbiztonságra költött források, illetve a kibertámadásokból fakadó károk terén, és várhatóan az aránytalanság is fennmarad. A kiberbiztonsági kiadások a következő években továbbra is elmaradnak a kívánatostól, és jelentős problémát okoz a források nem megfelelő, illetve nem kellően hatékony elköltése is, ami elvezet egy másik globális szintű kiberbiztonsági kihíváshoz. A kiberbiztonsági munkaerőpiacon az utóbbi időben egyre jelentősebbé váló anomáliákat az eddigi kihívásokhoz képest – azok összetettsége miatt – részletesebben mutatjuk be, több tanulmány alapján.

2014 nyarán a RAND Corporation kiadott egy tanulmányt *H4cker5 Wanted* címmel, amely alapvetően az Amerikai Egyesült Államok kiberbiztonsági munkaerejének helyzetével foglalkozott. Ha azonban elfogadjuk azt, hogy az Egyesült Államokat érintő infokommunikációs technológiákkal összefüggő folyamatok – ha némi késleltetéssel is, de – érzékelhetőek a világ más régióiban is, akkor a tanulmány megállapításai hasznosak lehetnek bármely ország számára. A tanulmány szerzői több korábbi jelentés és felmérés eredményét is feldolgozták, mint például az amerikai Kormányzati Ellenőrzési Hivatal (U.S. Government Accountability Office, GAO), az amerikai kormányzat számára tanácsadói tevékenységet folytató Booz-Allen Hamilton (BAH) vállalat, az amerikai Védelmi

Minisztérium (Department of Defense, DoD) vagy a Belbiztonsági Tanácsadó Testület (Homeland Security Advisory Council, HSAC). A GAO az azóta a történelem egyik legjelentősebb adatlopási incidensét elszenvedő kormányzati személyzeti irodával (Office of Personnel Management, OPM) közösen megfogalmazott több követendő gyakorlatot is a kiberbiztonsági munkaerő utánpótlásával kapcsolatban. A GAO munkatársai felhívták a figyelmet a nemzetbiztonsági átvilágításokból fakadó anomáliákra, amik miatt akár egy évig is elhúzódhatott egy felvételi procedúra, és listázták azokat a kormányzati kezdeményezéseket, amelyek a különböző állami szervezetek számára nyújtanak segítséget a megfelelő kiberbiztonsági munkaerő megtalálásában és képzésében (Libicki 2014, 14–17.).

Az OPM-hez hasonlóan ismerős lehet a Booz-Allen Hamilton vállalat neve is, mivel ez volt az a cég, amelyik munkaerő-kölcsönzés keretében Edward Snowdent kiközvetítette az amerikai Nemzetbiztonsági Szolgálathoz (National Security Agency, NSA), és aminek következtében 2013-ban Snowdennek lehetősége nyílt leleplezni az amerikai titkosszolgálatok tömeges megfigyelési gyakorlatát. A BAH is készített korábban egy gyakran hivatkozott tanulmányt arról, hogy milyen elvek és módszerek mentén lehetne erősíteni az amerikai szövetségi hivatalok kiberbiztonsági munkaerő-állományát. A tanulmány szerzői többek között megállapították, hogy az amerikai kormányzati kiberbiztonsági munkaerőprogramok széttagoltak, az OPM tevékenysége nem megfelelő, az alkalmazási szabályok túl komplexek, miközben a megbízásos szerződéssel történő alkalmazás jóval egyszerűbb. A szolgálatért kapott ösztöndíjprogramok sem jártak teljes sikerrel, az állami szervezetek pedig egymás elől vették el a kiberbiztonsági szakembereket, miközben továbbra sem jutott elegendő pénz kiberbiztonsági képzésre és humánerőforrás-fejlesztésre (Libicki 2014, 17–19.).

A Stratégiai és Nemzetközi Tanulmányok Központ (Center for Strategic and International Studies, CSIS) kiberbiztonsági munkaerővel foglalkozó elemzése alapvetően nem pénzügyi problémákat állapított meg az amerikai kormányzat szakemberhiányával kapcsolatban, sokkal inkább a menedzsment alacsony hatékonyságát hibáztatta a kialakult helyzetért. A legfontosabb javaslatok között szerepelt az amerikai Belbiztonsági Minisztérium (Department of Homeland Security, DHS) számára a kibertérhez kapcsolódó kormányzati szerepkörök és szakismeretek rendszertanának kialakítása, az amerikai Nemzeti Szabványügyi és Technológiai Intézet (National Institute of Standards and Technology) és más szereplők számára az engedélyezési követelményrendszer létrehozása, valamint az OPM számára a karrierstruktúra javítása (Libicki 2014, 19–22.).

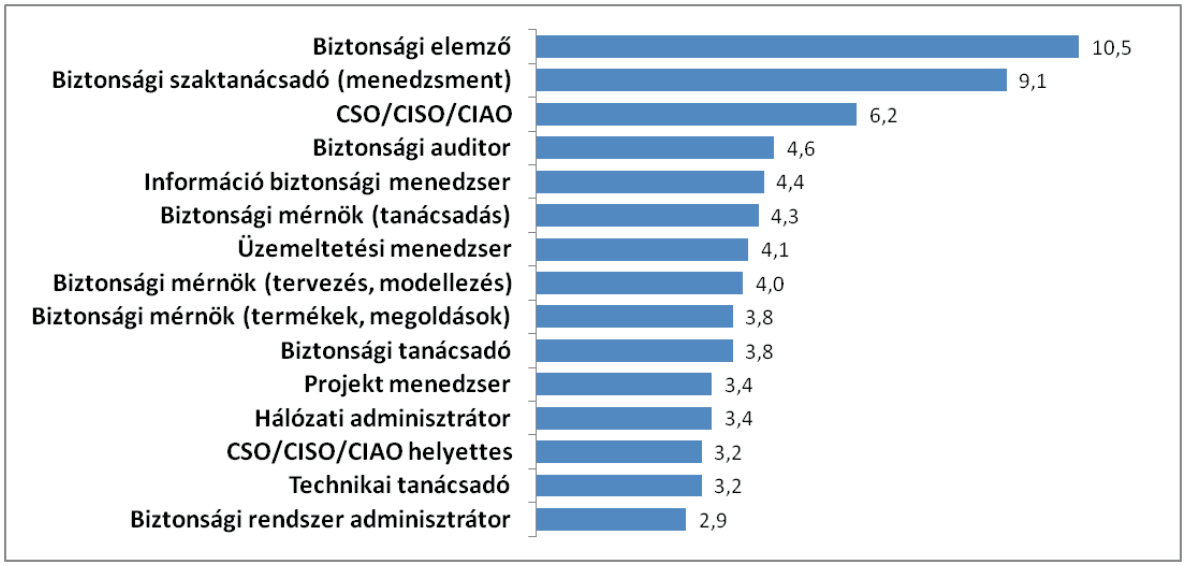
ADoD jelentése a kiberműveletek személyi állományáról jelentős hiányt mutatott ki a létszámban, illetve felhívta a figyelmet arra, hogy a különböző szolgálati ágak és haderőnemek eltérő igényekkel rendelkeznek a kiberbiztonsági szakértelem terén. Azért, hogy a DoD alá tartozó szervezetekben csökkenteni lehessen a kiberbiztonsági szakemberek hiányát, a minisztérium több programot is indított, amelyek elsősorban a képzési feltételek javítását és a pénzügyi körülmények fejlesztését szolgálták, például az iCollege program létrehozásával vagy a szakmai tanúsítványokért járó bónuszrendszer kialakításával (Libicki 2014, 22–24.).

A Belbiztonsági Tanácsadó Testület (HSAC) létrehozott egy munkacsoportot, aminek olyan kiemelkedő személyiségek is tagjai voltak, mint például a DEF CON hackerkonferencia alapítója, Jeff Moss vagy a SANS Intézet vezetője, Alan Paller. A testület arra jutott, hogy a Belbiztonsági Minisztérium (DHS) versenyképtelenné vált a munkaerőpiacon, mivel nem volt képes kellően érdekes és kihívásokkal teli munkát kínálni a kiberbiztonsági szakemberek számára. Az amerikai kormányzat számára megfogalmazott legfontosabb javaslataik a következők voltak:

- Irányadó lista elkészítése a kritikus kormányzati kiberbiztonsági feladatokról.
- Gyakorlati forgatókönyvek és egy értékelési modell kifejlesztése.
- Dedikált tanácsadói testület felállítása a kiberbiztonsági munkaerő fejlesztésére.
- A veteránok bevonása és egy kiberbiztonsági tartalékos program kialakítása (Libicki 2014, 24–25.).

A kiberbiztonsági feladatokat és a kapcsolódó munkaköröket általában egy kategóriába sorolva emlegetik, azonban a kiberbiztonsági pozíciók rendkívül szerteágazó tevékenységet fednek le, így

a szükséges szaktudás is eltérő. Bizonyos munkakörök betöltéséhez elengedhetetlen az erős technikai háttér, adott esetben a mérnöki végzettség, míg más esetekben inkább menedzsmentismeretekre és vezetői képességekre van szükség. Az (ISC)2 a világ legnagyobb, információ- és szoftverbiztonsági szakembereket tömörítő szervezete, mely több mint 160 országból 100 000-nél is több taggal rendelkezik. A szervezet által készített felmérés szerint 2015-ben a kiberbiztonság területén dolgozók több mint 10%-a biztonsági elemző volt, 9% körül alakult a biztonsági tanácsadók aránya, illetve meghaladta a 6%-ot a biztonsági és információbiztonsági vezetők aránya.

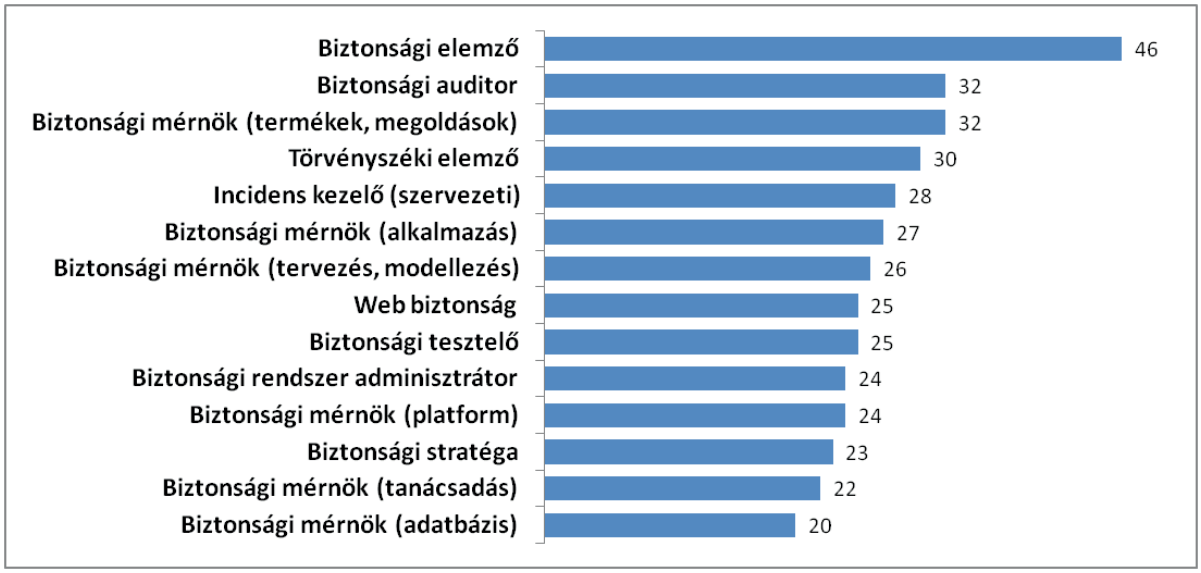


2. ábra

A Frost & Sullivan 14 000 válaszadóval készített felmérést az (ISC)2 számára, amiből következtetni lehet a globális viszonyokra is.

Forrás: Az eredeti forrás felhasználásával szerkesztette és fordította a szerző.
Az eredeti grafikon elérhető: www.isc2.org/2013-ISC2-Global-Information-Security-Workforce-Study.pdf
(a letöltés ideje: 2015. május 21.)

A felmérés készítői arra is kíváncsiak voltak, hogy azoknál a szervezeteknél, ahol a válaszadók dolgoznak, milyen kiberbiztonsági szakmákban van hiány, illetve mely pozíciók feltöltése okozza a legnagyobb kihívást. Az eredmények azt mutatják, hogy bár a válaszadók között is jelentős számban vannak a biztonsági elemzők, még többre lenne szükség. A legnagyobb, közel 50%-os igény a biztonsági elemzők iránt mutatkozik, de keresettek a biztonsági auditorok és azok a mérnökök is, akik a biztonsági termékek és megoldások tervezéséért felelősek.



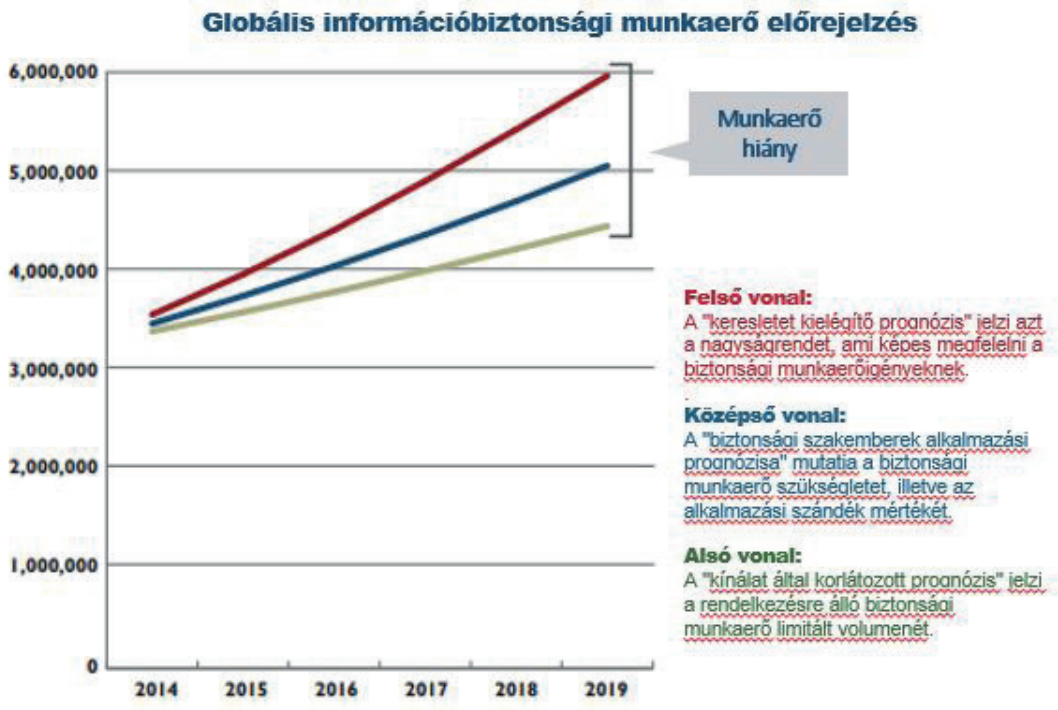
3. ábra

Az (ISC)2 számára készült 2015-ös felmérés alapján a legkeresettebb kiberbiztonsági szakmák sorrendje.

Forrás: Az eredeti forrás felhasználásával szerkesztette és fordította a szerző.
Az eredeti grafikon elérhető: www.isc2.org/2013-ISC2-Global-Information-Security-Workforce-Study.pdf
(a letöltés ideje: 2015. május 21.)

A válaszokból kitűnik, hogy jelentős igény van törvényszéki, illetve nyombiztosító elemzőkre, incidensek kezelésében jártas szakemberekre, de keresettek a biztonsági tesztelők, az adatbázisok, az alkalmazások és a különböző platformok biztonságához értő mérnökök is.

A 2015-ös felmérés alapján a készítők egy 2014 és 2019 közötti időszakra vonatkozó becslést is elvégeztek, amiből jól látszik, hogy a nagyjából 3,5 milliós szakemberlétszám 2019-re 4,5 millió körülire bővül, azonban az igények ennél jóval nagyobb mértékben fognak növekedni, és a kereslet várhatóan eléri a 6 millió főt globális szinten. A mintegy 1,5 millió fős különbség olyan kihívást jelent humán oldalról a kiberbiztonságban, amire ma még nem tudjuk biztosan a válaszokat. Amit viszont már most is biztosan tudunk, hogy erre a kihívásra nem lesz képes egyetlen ember vagy szervezet válaszokat adni. A kiberbiztonsági közösségnek és minden, a kibertérrel kapcsolatba kerülő szervezetnek, nemzetállamnak közre kell működnie abban, hogy a biztonság nagyobb figyelmet kapjon az átlag felhasználók körében éppúgy, mint a pályaválasztás előtt álló fiatalok esetében. A szükséges lépések késése vagy elmaradása csak ronthat a helyzeten.



4. ábra

A kiberbiztonsági munkaerő várható alakulása 2014 és 2019 között. (A zöld vonal jelöli azt a létszámot, ami biztosan megjelenik kínálati oldalon, a kék vonal mutatja az alkalmazási szándék várható alakulását, míg a vörös vonal azt jelzi, hogy mekkora lesz a teljes munkaerőigény a kiberbiztonság terén.)

Forrás: Az eredeti forrás felhasználásával szerkesztette és fordította a szerző.
Az eredeti grafikon elérhető: www.isc2.org/2013-ISC2-Global-Information-Security-Workforce-Study.pdf
(a letöltés ideje: 2015. május 21.)

Jól látható, hogy miközben a kiberbiztonsági munkaerőhiány minden szektort érint, még az Amerikai Egyesült Államok kormánya számára is komoly nehézségeket okoz a helyzet megoldása: rendszerszintű problémákkal kell szembenéznie, és bár a munkát más országok kormányaihoz képest jóval korábban megkezdték, úgy tűnik, 2015-ben még mindig rendkívül súlyos a helyzet. Elég csak a korábban már említett OPM adatlopási botrányára gondolni, amit 2015 júniusában fedeztek fel az illetékesek, és több mint 22 millió főt, az Egyesült Államok lakosságának 7%-át érintette az ügy (Zengerle–Cassella 2015). Szintén jelentős problémákra utal – még ha a forrás miatt fenntartásokkal is kell kezelnünk a hírt –, hogy az amerikai biztonsági rendszerek sérülékenységének napi szintű gyarapodásával még az ország legnagyobb riválisa, Kína sem tud lépést tartani, mert nem képes elég kiberbiztonsági szakembert biztosítani a felfedezett sérülékenységek kihasználásához (*Securing Our Future: Closing the Cybersecurity Talent Gap*, 2015). Szintén beszédes adatokat rejt a Raytheon amerikai védelmi ipari vállalat támogatásával az amerikai Nemzeti Kiberbiztonsági Szövetség (National Cyber Security Alliance, NCSA) által készített felmérés, ami elsősorban az Y generáció tagjai között vizsgálta a kiberbiztonsági szakma iránti érdeklődést. A felmérési eredményekből kitűnik, hogy a Közel-Keletet leszámítva minden régióban, illetve globálisan is 60% felett van azoknak a fiataloknak a száma, akik számára soha senki nem vetette fel annak lehetőségét, hogy kiberbiztonsági karriert építsenek. Ugyanakkor a válaszadók 38%-a szeretne többet tudni a kiberbiztonsági karrier lehetőségeiről. Szintén rendszerszintű problémára mutat rá, hogy globális szinten a fiatalok 58%-a nem részesült kiberbiztonsággal kapcsolatos formális oktatásban (China unable to recruit hackers fast enough to keep up with vulnerabilities in U.S. security systems. *The Onion,* 2016.).

A kiberbiztonsági munkaerőhiány kapcsán még 2015-ben napvilágot látott adatok szerint az Európai Unióban az ICT-szektor évente 120 000 új munkahelyet teremt. Azonban a magas munkanélküliség ellenére is, a képzett munkaerő hiánya miatt 2020-ra mintegy 900 000 ICT-állás maradhat betöltetlen az EU-ban. Tovább árnyalja a képet, hogy az EU lakosságának 20%-a soha nem használta az internetet, míg közel 40%-a nem rendelkezik megfelelő digitális képességekkel. Az EU lakóinak 14%-a pedig semmilyen digitális képességgel nem rendelkezik (Ansip 2015). Az önmagában alacsonynak tűnő érték valójában több mint 70 millió embert jelent. A még csak kialakulóban lévő helyzetre nincs azonnali megoldás. Bár sokan hisznek abban, hogy néhány év múlva a legtöbb kiberbiztonsági területen az emberek szerepét átveszi a gépi tanulás és a mesterséges intelligencia alkalmazása, ezeknek a megoldásoknak a széles körű elterjedése 2020 előtt nem várható, és azután sem lehet majd mindent funkciót gépekre bízni. A következő években nem várható, hogy hirtelen nagy számban jelennének meg kiberbiztonságban jártas, képzett munkavállalók a piacon, és ebben a kérdésben a bevándorlás és az agyelszívás sem jelent megoldást. Az egyetlen előremutató, hosszú távon is eredményt hozó megoldás az oktatás és a képzés, amihez nemzetközi összefogás szükséges annak érdekében, hogy a sokszor nagyon magas költségekkel képzett munkaerő ne hagyja el az adott országot vagy régiót. Jelenleg a nemzetközi kiberbiztonsági képzési és oktatási együttműködések meglehetősen fejletlenek – egy-két kivételtől eltekintve.

A nemzetközi együttműködések kapcsán gyakran felmerülő kihívás a terminológia kérdése. Bár elsőre nem tűnik komoly problémának, de ha jobban megvizsgáljuk a nemzetközi rendszer működésének alapjait és a különböző kooperatív kezdeményezéseket, hamar kiderül, hogy a kiberbiztonsági kihívások hatékony nemzetközi kezeléséhez nagy szükség lenne egy közös, egyezményes terminológia kialakítására. Ilyen azonban nem létezik, a kiberbiztonságnak nincs általánosan elfogadott meghatározása. Például az Európai Unió kiberbiztonsági stratégiája szerint a „kiberbiztonság azokat a biztosítékokat és intézkedéseket jelenti, amelyek segítségével mind a polgári, mind a katonai területeken egyaránt megvédhető a virtuális tér azoktól a fenyegetésektől, amelyek azok összefüggő hálózataival és információs infrastruktúráival kapcsolatosak vagy amelyek károsíthatják ezeket. A kiberbiztonság célja a hálózatok és az infrastruktúra rendelkezésre állásának és integritásának, valamint a benne lévő információk titkosságának megőrzése" (EU 2013, 3.). Az ENSZ mellett működő Nemzetközi Távközlési Egyesület (ITU) két meghatározása is érvényben van a kiberbiztonságra vonatkozóan. A rövidebb szerint az adatok és rendszerek védelmét jelenti azokon a hálózatokon, amelyek az internethez kapcsolódnak. A tömör definíció helyett érdemesebb inkább az ITU hosszabb meghatározását figyelembe venni, ami szerint a kiberbiztonság olyan eszközök, politikák, biztonsági koncepciók, útmutatások, kockázatkezelési törekvések, intézkedések, képzések, legjobb gyakorlatok és technológiák együttese, amelyek alkalmasak a kibertér, illetve a kibertérben működő szervezetek és személyek tulajdonának védelmére. A meghatározás kitér arra is, hogy a szervezetek és felhasználók tulajdona alatt kell érteni minden, a kibertérrel kapcsolatban álló eszközt, infrastruktúrát, alkalmazást, szolgáltatást, telekommunikációs rendszert és az összes küldött és tárolt információt.

Az ITU meghatározása magában foglalja az információbiztonság három alapelvét is: bizalmasság, sértetlenség, rendelkezésre állás (Mauer–Morgus 2014). Bizalmasság vagy titkosság alatt azt értjük, hogy az információhoz csak az előírt módon és csak olyan személyek férhetnek hozzá, akiket erre feljogosítottak. A sértetlenség vagy más néven integritás nem más, mint az adat és információ eredetisége és épsége, illetve az információs rendszer hiteles és pontos állapota. Egyszerűbben fogalmazva az adatokat és információkat csak azok módosíthatják, akik erre jogosultak, és véletlen változás nem fordulhat elő. A rendelkezésre állás szintén egy állapotot határoz meg, amely egyfelől állandóságot jelent, másfelől az adatok és információk meghatározott időben történő elérhetőségét. A rendelkezésre állást értelmezhetjük úgy is, hogy a felhasználót semmi nem akadályozza abban, hogy az adatokhoz és információkhoz hozzáférjen, amikor azokra szüksége van.

Ha már az euroatlanti szövetségi rendszer szóba került, érdemes megnézni a világ legerősebb katonai szervezeteként számon tartott NATO kiberbiztonsághoz kapcsolódó kifejezéseit. Katonai szervezet lévén a NATO által alkalmazott terminológia alapvetően a védelem és a kiber kifejezéseket

társítja, de szintén több meghatározás van használatban párhuzamosan. Az egyik szélesebb információbiztonsági környezetet foglal magában, ahol a kommunikációs és információs rendszerek biztonsága a bizalmasság, az integritás és a rendelkezésre állás megfelelő védelmének képességét jelenti. Ugyanakkor a NATO a kibervédelem kifejezés alatt olyan képességet ért, amivel egy műveleti kommunikációs és információs rendszer szolgáltatásai megvédhetők a kibertérből érkező rosszindulatú tevékenységekkel szemben (KLIMBURG 2012). Már az említett meghatározások nyomán is jól látható, hogy az egyes kiberbiztonsági definíciók között eltérés mutatkozik attól függően, hogy melyik szervezetről vagy intézményről van szó. A helyzet csak tovább bonyolódik, ha az egyes államok szintjén vizsgáljuk a kiberbiztonság meghatározását, mivel a legtöbb ország saját megfogalmazást, egyedi definíciót alkalmaz. Ezen a szinten az eltérések sokszor jelentéktelenek, de gyakran előfordulnak komoly különbségek is.

Mivel a fejezetnek nem célja a terminológiai hasonlóságok és eltérések részletes bemutatása, ezért az állami definíciók közül csak a magyar meghatározást mutatjuk be. A 2013-ban megjelent Nemzeti Kiberbiztonsági Stratégia (NKBS) 5. pontja az alábbiak szerint definiálja a kiberbiztonság fogalmát: „A kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez." (MK 2013, 6339.) A bemutatott meghatározások alapján jól látható, hogy a kiberbiztonság egyfelől leginkább egy állapotként írható le, amelynek három alapvető összetevője az adatok és információk bizalmassága, integritása és rendelkezésre állása, másfelől viszont egy olyan eszközrendszer, illetve képesség, amely a kibertérből eredő kockázatokat elfogadható szinten tudja tartani. Fontos megjegyezni, hogy a fizikai világhoz hasonlóan a kibertérben sem érhető el abszolút biztonság.

1.6. Kiberbiztonság a nemzetközi béke és biztonság tükrében

Az államok az 1990-es évek óta foglalkoznak az információs és telekommunikációs technológiák nemzetközi békére és biztonságra gyakorolt hatásaival. Az azóta eltelt időszakban számos jelentős kiberbiztonsági incidens történt, melyek miatt a kormányok új politikákat és szervezeteket kezdtek el kialakítani a kibertér katonai célú felhasználásával összefüggésben. Ennek eredményeként jelenleg is aktív vita folyik arról, hogy milyen nemzetközi normák mentén lehetne irányítani a kiberteret, és milyen módon lehetséges a bizalomépítés ebben a dimenzióban. Fontos lenne a stabilitás növelése, illetve az államok számára olyan kiberbiztonsági képességek kialakítása, amelyek segítségével hatékonyan léphetnek fel a kibertérből érkező kihívásokkal szemben saját határaikon belül és kívül egyaránt. Az elmúlt évek trendjei alapján számos ország kezdte el a kiberbiztonsági kérdéseket beépíteni a nemzeti biztonsági és védelmi stratégiákba, illetve a fejlett államok mára már önálló stratégia keretén belül foglalkoznak a kibertér biztonságának garantálásával.

A politika legfelső szintjeire eljutó kiberbiztonsági kérdések nyomán nemzeti beruházások indulnak annak érdekében, hogy kibervédelmi vagy éppen támadó képességeket alakítsanak ki a kihívások és sérülékenységek kezelésére. A fokozott érdeklődésnek és beruházásoknak köszönhetően újabb kérdések merülnek fel, például a hagyományos biztonsági koncepciók alkalmazhatóságával, a kibertérre vonatkozó joggal és a kibertér irányítási struktúrájával kapcsolatban. A kialakult párbeszédek fókuszában jellemzően a nemzetközi jog alkalmazhatósága, a kibertérre vonatkozó normák és az államok kibertérben tanúsított magatartási formái állnak. Ezen a téren az egyik meghatározó politikai irány a tömegpusztító fegyverek leszereléséhez kapcsolódó bizalom és biztonságerősítő intézkedések nyomán próbálja meg a kiberteret biztonságosabbá tenni és az ehhez szükséges kibervédelmi kapacitásokat kialakítani. A fizikai világra alkalmazott nemzetközi jog, illetve az annak részét képező hadijogi alapelvek kapcsán fontos kérdések merülnek fel: például hogy a megkülönböztetés vagy az arányosság elve miként alkalmazható a kibertérben. A megkülönböztetés koncepciója szerint

a hadviselő feleknek különbséget kell tenniük civil és katonai célpontok között, ami jelenleg szinte egyáltalán nem kivitelezhető a kibertérben. Hasonlóan problémás terület az arányosság elve, amelynek értelmében a támadással okozott pusztításnak arányban kell lennie a katonai előnnyel, amire a támadás következtében tesz szert valamely hadviselő fél. Tekintettel arra, hogy ezek az elvek nehezen vagy csak megkötésekkel alkalmazhatók a kibertérre, több olyan javaslat is napvilágot látott, amelyek értelmében a kibertérben megnövekedne az állam szerepe az információk ellenőrzése terén. Ezek az erőfeszítések azonban jelentős veszélyeket hordoznak magukban, elsősorban a szólásszabadságra. Ez az egyik oka annak, hogy az információbiztonság és a kiberbiztonság meghatározása és a kapcsolódó, egységes terminológia kialakítása során fontos emberi jogi kérdésekre is tekintettel kell lenni. Szintén fontos, hogy ezeknek a jelentős kérdéseknek a megvitatása korábban a nemzetállamok kiváltsága volt, a kibertérben azonban a társadalmi szereplőknek nem csak közvetett módon lehet nagy hatása a nemzetközi békére és biztonságra. A kiberbiztonság aktualitásairól számos fórumon értekeztek már a nemzetközi béke és biztonság perspektíváit szem előtt tartva, azonban a kibertér védelmét és biztonságát erősíteni hivatott nemzetközi együttműködések a mai napig gyerekcipőben járnak. A kooperatív kezdeményezések túlnyomórészt egyetlen régióra vagy valamilyen problémakörre próbálnak megoldást találni. Kérdés, hogy a fragmentáltság a hatékonyságot milyen mértékben befolyásolja egy olyan határok nélküli közegben, ahol minden mindennel összefügg…

Felhasznált irodalom

Ansip, Andrus (2015): *Digital skills, jobs and the need to get more Europeans online.* Elérhető: https://ec.europa.eu/commission/commissioners/2014-2019/ansip/blog/digital-skills-jobs-and-need-get-more-europeans-online_en (a letöltés ideje: 2017. április 2.)

Berzsenyi Dániel – Ványi Rajmond: Egy katonapolitikai döntés lehetséges kiberbiztonsági következményei. *Nemzet és Biztonság,* 8. évf. 3. sz.134–143. Elérhető: http://nemzetesbiztonsag.hu/cikkek/nb_2015_3_12_berzsenyi-vanyi_-_egy_katonapolitikai_dontes_lehetseges_kiberbiztonsagi_kovetkezmenyei_iszlam_allam.pdf (a letöltés ideje: 2015. december 27.)

China unable to recruit hackers fast enough to keep up with vulnerabilities in U.S. security systems. *The Onion,* 2016. Elérhető: www.theonion.com/article/china-unable-recruit-hackers-fast-enough-keep-vuln-51719 (a letöltés ideje: 2015. október 26.)

Evans, Dave (2011): *The Internet of Things. How the Next Evolution of the Internet Is Changing Everything.* Cisco,Elérhető: http://blogs.cisco.com/diversity/the-internet-of-things-infographic (a letöltés ideje: 2014. április 21.)

Hart, Kim (2008): Longtime Battle Lines Are Recast In Russia and Georgia's Cyberwar. *Washington Post.* Elérhető: www.washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623.html?hpid=topnews (a letöltés ideje: 2017. április 2.)

ICT Facts and Figures 2016. ITU. Elérhető: www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf (a letöltés ideje: 2016. október 19.)

IoT: Hottest technology to watch out for in 2015. *The Economic Times,* 2015. Elérhető: http://economictimes.indiatimes.com/news/industry/jobs/iot-hottest-technology-to-watch-out-for-in-2015/articleshow/45807138.cms (a letöltés ideje: 2015. október 8.)

Klimburg, Alexander ed.(2012): *National Cyber Security Framework Manual.* Elérhető: https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf (a letöltés ideje: 2013. december 2.)

Kovács László – Krasznay Csaba (2017): Mert övék a hatalom. *SVKK Elemzések*. Elérhető: http://netk.uni-nke.hu/uploads/media_items/svkk-elemzesek-2017-9-az-internet-politikat-is-befolyasolo-hatasa-a-2016-os-amerikai-elnokvalasztas-soran-kovacs-l-krasznay-cs.original.pdf (a letöltés ideje: 2017. május 5.)

Libicki, Martin C. – Senty, David – Pollak, Julia (2014): *H4cker5 Wanted. An Examination of the Cybersecurity Labor Market.* RAND Corporation. Elérhető: http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf (a letöltés ideje: 2014. június 23.)

Maurer, Tim – Morgus, Robert (2014): *Compilation of Existing Cybersecurity and Information Security Related Definitions.*Elérhető: https://na-production.s3.amazonaws.com/documents/compilation-of-existing-cybersecurity-and-information-security-related-definitions.pdf (a letöltés ideje: 2015. február 19.)

Measuring the Information Society, 2012. ITU. Elérhető: www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf (a letöltés ideje: 2016. október 22.)

MÉSZÁROS Csaba (2016): Fenyegetések Internete. *Computerworld.* Elérhető: http://computerworld.hu/computerworld/fenyegetesek-internete.html (a letöltés ideje: 2017. január 12.)

MORGAN, Steve (2016): *2016 Cybercrime Report.* Cybersecurity Ventures. Elérhető: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (a letöltés ideje: 2017. február 17.)

Overview of the Internet of Things, 2012. ITU. Elérhető: www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060 (a letöltés ideje: 2014. április 21.)

Rendszeres internethasználók aránya (2005–2016). KSH. Elérhető: www.ksh.hu/docs/hun/eurostat_tablak/tabl/tin00091.html (a letöltés ideje: 2016. október 19.)

RETTMAN, Andrew (2017): German spy chief warns Kremlin on election hack. *Euobserver.* Elérhető: https://euobserver.com/foreign/137788 (a letöltés ideje: 2017. május 6.)

Securing Our Future: Closing the Cybersecurity Talent Gap. Raytheon, 2015. Elérhető: www.staysafeonline.org/download/datasets/16847/Securing%Our%Future%Closing%the%Cybersecurity%Talent%Gap.pdf (a letöltés ideje: 2016. október 30.)*Symantec Internet Security Threat Report, 2017.* Elérhető: www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf (a letöltés ideje: 2017. május 4.)

The Internet of Everything: 2014. *Business Insider.* Elérhető: www.businessinsider.com/the-internet-of-everything-2014-slide-deck-sai-2014-2#-11 (a letöltés ideje: 2016. október 22.)

WIRTZ, James J. (2015): *Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy.* CCDCOE. Elérhető: https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Wirtz_03.pdf (a letöltés ideje: 2016. november 2.)

World Population Prospects. The 2015 Revision. UN. Elérhető: https://esa.un.org/unpd/wpp/publications/files/key_findings_wpp_2015.pdf (a letöltés ideje: 2016. október 19.)

ZENGERLE, Patricia – CASSELLA, Megan (2015): Millions more Americans hit by government personnel data hack. *Reuters.* Elérhető: www.reuters.com/article/us-cybersecurity-usa-idUSKCN0PJ2M420150709 (a letöltés ideje: 2015. július 10.)

2. A BIZTONSÁGI ESEMÉNYEK ÉS AZ ADATVÉDELMI INCIDENSEK KEZELÉSÉRE VONATKOZÓ ELŐÍRÁSOK HAZÁNK ÉS AZ EU JOGÁBAN

Dr. Kiss Attila

2.1. A biztonsági események jogi jelentősége

2.1.1. Bevezető gondolatok

Már az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) preambuluma rögzíti, hogy az állam és polgárai számára kiemelt jelentőségű az elektronikus információs rendszerekben[1] kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint az információs rendszerelemek sértetlenségének és rendelkezésre állásának garantálása. A törvény hatálya alá tartozó információs rendszerek üzemeltetői, kezelői és az azok biztonságáért felelős személyek tehát kötelesek egyrészt a nemzeti elektronikus adatvagyon részét képező rendszereik zárt, teljes körű, folytonos és a kockázatokkal arányos védelmére, másrészt felelősek azért is, hogy garantálják azoknak a polgároknak (érintetteknek) a jogait, akikről a rendszer adatot kezel.

Számos hazai és nemzetközi dokumentum rendelkezik e két elvárás összekapcsolásáról, amikor az érintett magánéletének tiszteletben tartásához fűződő jogának elemeként rögzíti kommunikációjának bizalmas jellegét és személyes adatai védelemét.[2] A hatályos adatvédelmi szabályozás is több helyen foglalkozik e bizalmas jelleg fenntartásával, mind jogi, mind biztonsági megközelítésből. Személyes adatot[3] kezelni – beleértve az adatok elektronikus (és papíralapú) rögzítését, gyűjtését, tárolását, továbbítását, vagy bármilyen célú felhasználását is – ugyanis csak az érintett magánszemélyek jogainak tiszteletben tartásával lehet. Ebbe beletartozik az adatkezelő arra vonatkozó kötelezettsége is, hogy megfeleljen az adatok kezelésének információbiztonsági elvárásainak.

E fejezet célja ezért az, hogy bemutassa az elektronikus információs rendszerek biztonságáért felelős személyek előtt álló kihívásokat és a rájuk vonatkozó előírásokat abban az esetben, ha a fenti követelmény nem teljesül, tehát biztonsági esemény következik be. Az Ibtv. meghatározása szerint biztonsági esemény *„az a nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely*

---

[1] Az Ibtv. 1. § (1) bekezdés 14b. pontja alapján: „Az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese."

[2] Az Emberi Jogok Európai Egyezményének 8. cikke; a lisszaboni szerződéssel 2009-ben elfogadott Európai Unió Alapjogi Chartájának 7. és 8. cikke; valamint az EU adatvédelmi irányelve, amely például az ezek által nevesített alapjogok védelmét, beleértve az adatok biztonságának garantálását is, előírja. (A személyes adatok feldolgozása kérdésében az egyének védelméről és az ilyen adatok szabad áramlásáról szóló európai parlamenti határozat és a Tanács 95/46/EK irányelve rendelkezik.) Továbbá az EU Digitális Menetrendje, de a magyar Alkotmánybíróság több határozata és adatvédelmi tárgyú törvényeink is szabályozzák ezt a kérdést.

[3] Az Infotv. 3. § 2. pont megfogalmazása szerint személyes adat „az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés."

az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül".[4]

Abban az esetben, ha feltételezhető, hogy az eseményben érintett információ személyes adatot is tartalmaz (vagy tartalmazott), akkor a biztonságért felelős személy nagy valószínűséggel egyben egy adatvédelmi incidenst észlelt, tehát köteles a lehető legrövidebb időn belül az incidens kezelésére (ha lehetséges az érintettekre nézve bekövetkező károk mérséklésére). Az adatvédelmi incidens fogalmát az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) értelmező rendelkezései között találjuk: *„Személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés."*[5] Szerencsés esetben, ha az adott szervezet vezetője az Infotv. szerint köteles belső adatvédelmi felelős kinevezésére,[6] vagy kijelöléséről önként rendelkezett, akkor a biztonsági felelős vagy vezető őt segítségül hívhatja,[7] de így is feladata marad az incidens felismerése, jellegének, hatókörének felmérése.

A biztonsági eseményekhez kötődő feladatok vizsgálatának különös aktualitást ad, hogy 2018 májusától az Európai Unió szabályozása tovább egységesíti az egyes tagállamokban bevett eseménykezelési gyakorlatot. A 2020-ig tartó jogalkotási stratégia keretében számos olyan, a digitális térbe vetett bizalom fejlesztését szolgáló rendelkezést dolgoztak ki, amelyek együttműködésre ösztönzik a biztonsági felelősöket, és megkísérlik hatékonyabbá tenni a felügyeleti intézményrendszert. A 2012 óta tartó reformfolyamat eredményeként elfogadott jogszabályok közül ki kell emelnünk a 2018. május 25-től alkalmazandó 2016/679/EU Általános Adatvédelmi Rendeletet (a továbbiakban: GDPR),[8] valamint a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016/1148/EU irányelvet (a továbbiakban: NIS irányelv). E két jogszabály közvetlenül is hatással van a hazai jogban rögzített feladatokra, számos újdonságot hoz a biztonsági eseménykezelés területén is, ezért külön cím alatt vizsgáljuk ezek legfontosabb előírásait. A fejezet emellett áttekintést nyújt a legfontosabb kapcsolódó fogalmakról, jogszabályi rendelkezésekről és az ezek alkalmazásával kapcsolatos kihívásokról.

2.1.2. A kapcsolódó fogalmak áttekintése

Az elektronikus információs rendszereket érintő fenyegetések napjainkra állandósultak. Szinte naponta derül fény egyes szolgáltatások előfizetőit vagy olykor a lakosság jelentős részét érintő adatszivárgásokra, adatvesztésekre,[9] esetleg kórházakat vagy kormányzati oldalakat célzó támadásokra. Ez annak tükrében különösen meglepő, hogy a biztonsági események körében magas a látencia, sok esetről csak jelentős késéssel vagy sosem értesülnek a rendszerek üzemeltetői. A szervezeteik jó hírnevét féltő vezetők körében szintén nem túl népszerű intézkedés az incidensek nyilvánosságra hozatala, az abban érintett magánszemélyek tájékoztatása, mivel az ilyen események bekövetkezése rosszul hathat a szervezet megítélésére. Így általában csak akkor választják ezt a megoldást az adatkezelő szervek, személyek, ha már nyilvánvalóvá válik az okozott probléma. Ezért a támadások megelőzése,

---

[4] Ibtv. 1. § (1) bekezdés 9. pont.

[5] Infotv. 3. § 26. pont.

[6] Infotv. 24. § (1).

[7] Baranya Zsolt azonban kifejti, hogy jelenleg sem példa nélküli, és a 2018-tól alkalmazandó előírások sem zárják ki, hogy az adatbiztonsági felelősi és a belső adatvédelmi felelősi feladatokra azonos személyt nevezzen ki a szervezet vezetője, sőt, a feladatokhoz szükséges intézkedések akár hatékonyabban is megvalósíthatóak lehetnek az informatikai és jogi kompetenciával is rendelkező szerepkör miatt. (Baranya 2016)

[8] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (Általános Adatvédelmi Rendelet). Nemzetközileg bevett rövidítése GDPR, az angol elnevezése után: *General Data Protection Regulation.*

[9] Lásd például: www.databreaches.net (a letöltés ideje: 2017. április 30.)

elhárítása, az ehhez szükséges hatékony fizikai és a virtuális térben történő biztonsági kontrollok kialakítása, az események észlelési és bejelentési gyakorlatának kialakítása költséges és időigényes mind a rendszer tulajdonosai – legyen az állami vagy piaci szereplő –, mind az üzemeltetői, biztonsági felelősök számára.

Az adatszivárgások, visszaélési botrányok magas száma jól mutatja, hogy önmagában a szabályozás, az önszabályozás és a jogalkalmazás sem tud elegendő védelmet nyújtani a felhasználóknak a tömegesen előforduló visszaélésekkel szemben. Ugyanakkor az adatkezelők sem lehetnek biztonságban az egyre újabb, a támadók számára értékes (személyes) adatok megszerzésére tervezett műszaki és *social engineering* típusú támadások ellen.

A kiberbiztonság fogalma alatt egy átfogó jellegű tevékenységi kört értünk, egy olyan komplex intézkedésrendszert, amely a biztonság értelmezéséből kiindulva minden lehetséges eszközt igénybe vesz a kibertérben létező kockázatok kezelésére. Ide sorolhatjuk a politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazását is, amelyek – a kibertérben létező kockázatok elfogadható szintjét biztosítva – a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.[10]

A 2013 márciusában kiadott Nemzeti Kiberbiztonsági Stratégia[11] a magyar nemzeti kibertér biztonsága szempontjából legfontosabb megelőzési, észlelési, kezelési (reagálási), válaszadási és helyreállítási képességek kiépítését segíti elő. A dokumentum átfogó jelleggel határozza meg a magyar kiberteret érintő rossz szándékú kibertevékenység, -fenyegetés, -támadás, illetve -vészhelyzet, valamint a vétlen információszivárgás csökkentése, elhárítása érdekében alkalmazható kibervédelem állami eszközeit.

A stratégiában meghatározott célok érvényesülését nagyban elősegíti az a tény, hogy ennek előírásait a közigazgatás, a létfontosságú rendszerek és más kritikus infrastruktúrák kezelői számára törvénybe iktatták, az Ibtv.-vel kötelező jogi előírássá tették.

A törvénynek a bevezetőben ismertetett preambulumából kiolvasható a fenyegetés, a biztonság és a védelem fogalmának jelentősége. A fenyegetéseket, tehát a még be nem következett, de lehetséges eseményeket az Ibtv. általánosítva úgy határozza meg, mint „*olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát”*.[12]

Az elektronikus információs rendszer biztonsága alatt a törvény azt az állapotot érti, amelyben a védelem mint tevékenység az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása mint védendő értékek szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.[13] Azaz a védelem megvalósítása során az összes számításba vehető fenyegetést kell figyelembe venni, úgy, hogy a védelem az elektronikus információs rendszer valamennyi elemére kiterjed, folyamatában megvalósul, továbbá költségei arányosak a fenyegetések által okozható károkkal. Ez alatt azt értjük, hogy egy kellően nagy időintervallumban a védelem költségei arányosak a feltételezhető kárértékkel, azaz a védelemre akkora összeget és oly módon fordítanak, hogy ezzel a kockázat a védő számára még elviselhető mértékű vagy annál kisebb legyen (Muha–Krasznay 2014).

A biztonság tehát egy olyan statikus állapot, amely megfelel a kockázatelemzésen alapuló, várható fenyegetésekkel szemben elérni kívánt biztonsági szintnek, amely együttesen nem más, mint a védelmi intézkedések által kifejtett hatások összessége. A kívánt biztonsági szint eléréséhez és fenntartásához tehát tervezett védelmi intézkedések sokaságát kell megtenni, azaz a védelmi rendszer megfelelő állapotát szükséges biztosítani. A védelem ebben az értelemben tehát nem más, mint a fenyegetések ellen

[10] Ibtv. 1. § (1) bekezdés, 26. pont.
[11] 1139/2013. (III. 21.) kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.
[12] Ibtv. 1. § (1) bekezdés, 119. pont.
[13] Ibtv. 1. § (1) bekezdés, 15. pont.

hozott tevékenységek és intézkedések összessége, amelyek által lehetőleg elkerülhető lesz a biztonsági események bekövetkezése. Az Ibtv. az alábbi védelmi formákat nevesíti:

- adminisztratív védelem, azaz szervezési, szabályozási, ellenőrzési intézkedések összessége és az oktatás,[14]
- fizikai védelem, azaz a fizikai térben megvalósuló fenyegetések elleni intézkedések rendszere, ide sorolva a természeti csapás elleni és a mechanikai, az élő erős védelmet, az elektronikai jelzőrendszert, a beléptető és a megfigyelő rendszert, a tápáramellátást, a sugárzott és vezetett zavarvédelmet, a klimatizálást és a tűzvédelmet,[15]
- logikai védelem, azaz az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem.[16]

Ha a fenyegetések ellen felépített védelmi intézkedések nem érik el a kívánt hatást, vagy sérül a rendszer – meghibásodás vagy vis major, illetve szándékosság esetén –, olyan események vagy eseménysorozatok következhetnek be, amelyek kezelése eltérő működést kíván az elektronikus információs rendszer üzemeltetőjétől, az egyéntől, a szervezettől, amely működést – különleges szerepe miatt – szabályozási oldalról (is) szükséges kezelni.

2.1.3. A biztonsági esemény tulajdonságai

Az Ibtv.-ben önálló fogalomként jelenik meg a *bizalmasság,*[17] a *sértetlenség*[18] és a *rendelkezésre állás.*[19] Ezen tulajdonságok sérülése vezet a bevezetőben meghatározott biztonsági esemény bekövetkeztéhez. Az értelmező rendelkezések az alábbiakat rögzítik:

- Bizalmasság alatt az elektronikus információs rendszer azon tulajdonságát kell érteni, amely szerint az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek annak felhasználásáról.
- Sértetlenségen az adat azon tulajdonságát kell érteni, amely szerint:
  - az adat tartalma és tulajdonságai az adattal szemben felállított követelményekkel megegyeznek, az adat az elvárt forrásból származik, azaz hiteles,
  - az adat származása, azaz eredete ellenőrizhető (letagadhatatlan); sértetlenség továbbá az elektronikus információs rendszer elemeinek azon tulajdonsága is, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.
- Rendelkezésre állás alatt annak biztosítását kell érteni, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak.

A hatályos szabályozási környezet megkülönbözteti a biztonsági esemény fogalmát a súlyos biztonsági esemény fogalmától. *Súlyos biztonsági eseménynek*[20] kell tekinteni azt az informatikai eseményt, amelynek bekövetkezése esetén:

- az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet,
- emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be,

[14] Ibtv. 1. § (1) bekezdés, 6. pont.
[15] Ibtv. 1. § (1) bekezdés, 20. pont.
[16] Ibtv. 1. § (1) bekezdés, 34. pont.
[17] Ibtv. 1. § (1) bekezdés, 8. pont.
[18] Ibtv. 1. § (1) bekezdés, 39. pont.
[19] Ibtv. 1. § (1) bekezdés, 38. pont.
[20] Ibtv. 1. § (1) bekezdés, 41. a pont.

- súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben,
- alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek.

Az Ibtv. az első pontban említett kritikus adatnak[21] az adatvédelmi törvényben (Infotv.) meghatározott személyes adatot, különleges adatot[22] vagy valamely egyéb jogszabállyal védett adatot tekinti. Utóbbi védett adatok körébe tartozik például a minősített adat védelméről szóló 2009. évi CLV. törvény értelmező rendelkezései által meghatározott nemzeti vagy külföldi minősített adat,[23] melyek megsértése szabálysértési vagy büntetőeljárás lefolytatását vonhatja magával. A személyes vagy különleges adatokat érintő biztonsági esemény emellett megvalósíthatja az Infotv.-ben említett adatvédelmi incidens fogalmát is, ezért az adatvédelmi szabályozásban rögzített felelősséget, illetve teendőket is az adatkezelő szervezetnek kell vállalnia.

Elektronikus információs rendszereknél *kiemelkedően nagy káresemény* következhet be, ha az Ibtv. előírásait kiegészítő végrehajtási rendelet, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és a biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet (a továbbiakban: BM rendelet) 1. mellékletének 2. pontja szerint az 5. biztonsági osztályba sorolt rendszerben következik be a biztonsági esemény, mivel annak következtében:

- kiemelten nagy mennyiségű különleges személyes adat sérülhet;
- emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be;
- a nemzeti adatvagyon helyreállíthatatlanul megsérülhet;
- az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított;
- a lehetséges társadalmi-politikai hatás következtében súlyos bizalomvesztés lép fel az érintett szervezettel szemben, alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek,
- az üzlet- vagy ügymenet szempontjából nagy értékű, üzleti titkot vagy kiemelten érzékeny folyamatokat kezelő elektronikus információs rendszer vagy információt képező adat tömegesen vagy jelentősen sérülhet;
- a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 15%-át.

Tehát súlyos biztonsági esemény bekövetkezésével a legmagasabb, 5. biztonsági osztályba sorolt elektronikus információs rendszer esetében kell számolnunk.

Egy adott biztonsági esemény bekövetkezését követően a kiváltott hatásnál figyelembe kell venni, hogy az milyen időtartamban állt fenn, milyen kiterjedtségű volt – akár földrajzi értelemben is –, milyen mértékű problémát, zavart okozott (adott esetben az elektronikus információs rendszer működésén túl az állam, a társadalom és a gazdaság tevékenységében), hány felhasználót és/vagy szolgáltatást érintett. A kiváltott hatás befolyásolja a választandó eseménykezelést is.

[21] Ibtv. 1. § (1) bekezdés, 32. a pont.

[22] Az Infotv. 3. § 3. pontja értelmében különleges adat: „A faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, valamint az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat."

[23] A minősített adat védelméről szóló 2009. évi CLV. törvény 3. § 1. pontja szerint.

2.1.4. Az események kezelésére vonatkozó előírások

2.1.4.1. Az Ibtv. által rögzített feladatok

Ha biztonsági eseményre kerül sor, akkor intézkedni kell annak azonnali és hatékony kezeléséről, annak érdekében, hogy az újbóli vagy megismételt biztonsági események bekövetkezésének valószínűsége csökkenjen, a bekövetkező kár minimalizálható legyen. Az Ibtv. a biztonsági események kezelését fogalmi szinten határozza meg, ezekre kell értelmeznünk az adminisztratív, a fizikai és a logikai védelmi intézkedéseket:

- dokumentálás,
- a következmények felszámolása,
- a bekövetkezés okainak és felelőseinek megállapítása és
- a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység.[24]

A törvény rögzíti, hogy az eseménykezelés történhet:

- a védelmi intézkedések kiegészítésével vagy megerősítésével,
- a szabályozás javításával,
- az érintettek oktatásával és
- egyéb módon is.

Az Ibtv. – a kapcsolódó nemzetközi szabványokhoz hasonlóan – alapvető követelményként rögzíti,[25] hogy az intézkedéseknek a biztonsági események kezelése mellett – a PreDeCo (Preventive–Detective–Corrective, azaz megelőz, feltár, javít) elvet alapul véve – támogatniuk kell:

- a megelőzést, azaz a fenyegetés által okozható hatás bekövetkezésének elkerülését,[26]
- a korai figyelmeztetést, azaz olyan aktív szervezeti cselekvést, amelynek során valamely fenyegetés várható bekövetkezésének jelzésére kerül sor a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni,[27]
- az észlelést, azaz a biztonsági esemény bekövetkezésének felismerését[28] és
- a reagálást, amely a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedéseket foglalja magában.[29]

2.1.4.2. Intézkedések meghatározott osztályok alapján

A BM rendelet 3. melléklete[30] az adminisztratív védelmi intézkedések között rögzíti a biztonsági események kezelésre vonatkozó követelményeket. Az intézkedések az adott elektronikus információs rendszer biztonsági osztályba sorolt értékének növekedésével arányosan szigorodnak: magasabb osztályba sorolt érték esetén egyre összetettebb védelmi intézkedéseket igényelnek a szervezet részéről. A BM rendelet az eseménykezelésben az 1. és 2. biztonsági osztályra nem rögzít önálló adminisztratív védelmi intézkedéseket.

[24] Ibtv. 1. § (1) bekezdés, 10. pont.
[25] Ibtv. 6. §.
[26] Ibtv. 1. § (1) bekezdés, 36. pont.
[27] Ibtv. 1. § (1) bekezdés, 32. pont.
[28] Ibtv. 1. § (1) bekezdés, 17. pont.
[29] Ibtv. 1. § (1) bekezdés, 37. pont.
[30] BM rendelet, a 3. melléklet 2. alcíme alatt szereplő táblázat 3.1 alpontjának 3.1.5. alpontja.

2.1.4.3. A 3. biztonsági osztálytól kötelező intézkedések köre

- Biztonsági eseménykezelési eljárásrend készítése.
  1. A szervezet kötelezettsége, hogy a biztonsági eseményekre olyan *eseménykezelési eljárásrendet dolgozzon ki,* amely a PreDeCo elvet felhasználva magába foglalja az előkészületet, az észlelést, a vizsgálatot, az elszigetelést, a megszüntetést és a helyreállítást.
  2. A szervezetnek *a kidolgozott eseménykezelési eljárásokat egyeztetnie kell az üzletmenet-folytonossági tervéhez tartozó tevékenységekkel.* Az üzletmenet (ügymenet) folytonosságának tervezése során elkészített eljárásrendben[31] az informatikai erőforrások kiesésének esetére köteles összehangolni a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével.
  3. A szervezetnek *az eseménykezelési tevékenységekből levont tanulságokat be kell építenie az eseménykezelési eljárásokba,* a fejlesztési és üzemeltetési eljárásokba és elvárásokba, a továbbképzésekbe és a tesztelési folyamatokba.
- Biztonsági események figyelése: a szervezet nyomon követi és dokumentálja az elektronikus információs rendszer biztonsági eseményeit.
- Biztonsági események jelentése: a szervezet minden szereplőtől, amely az elektronikus információs rendszerrel vagy azok elhelyezésére szolgáló objektummal kapcsolatban áll, megköveteli, hogy jelentsék a biztonsági esemény bekövetkeztét vagy ha erre utaló jelet, veszélyhelyzetet észlelnek. A szervezet a biztonsági eseményekre vonatkozó információkat a jogszabályban meghatározottak szerint jelenti az elektronikus információs rendszerek biztonságának felügyeletét ellátó szerveknek.
- Segítségnyújtás a biztonsági események kezeléséhez. A szervezet tanácsadást és támogatást nyújt az elektronikus információs rendszer felhasználóinak a biztonsági események kezeléséhez és jelentéséhez.
- Biztonsági eseménykezelési terv készítése.
  1. A szervezet kötelezettsége, hogy biztonsági eseménykezelési tervet dolgozzon ki, amely:
     – iránymutatást tartalmaz a biztonsági esemény kezelési módjaira,
     – ismerteti a biztonsági eseménykezelési lehetőségek struktúráját és szervezetét,
     – átfogó megközelítést nyújt arról, hogy a biztonsági eseménykezelési lehetőségek hogyan illeszkednek az általános szervezetbe,
     – tartalmazza a szervezet feladatkörével, méretével, szervezeti felépítésével és funkcióival kapcsolatos egyedi igényeket,
     – meghatározza a bejelentésköteles biztonsági eseményeket,
     – meghatározza és folyamatosan pontosítja a biztonsági események értékelésének, kategorizálásának (például súlyosság) kritériumrendszerét,
     – támogatást ad a biztonsági eseménykezelési lehetőségek belső mérésére,
     – meghatározza azokat az erőforrásokat és azt a vezetői támogatást, amelyek szükségesek a biztonsági eseménykezelési lehetőségek bővítésére, hatékonyabbá tételére és fenntartására.
  2. A szervezet kihirdeti és ismerteti a biztonsági eseménykezelési tervet – ideértve annak változásait is – a biztonsági eseményeket kezelő (névvel és/vagy szerepkörrel azonosított) személyeknek és szervezeti egységeknek, nyilatkoztatja őket annak tudomásulvételéről.
  3. A szervezet kötelezettsége, hogy a biztonsági eseménykezelési tervet:
     – meghatározott gyakorisággal felülvizsgálja,
     – frissítse, figyelembe véve az elektronikus információs rendszer és a szervezet változásait vagy a terv megvalósítása, végrehajtása és tesztelése során felmerülő problémákat.

[31] BM rendelet 4. melléklet, 3. alcím 3.1.4. alpontja.

4. A szervezet kötelezettsége gondoskodni arról, hogy a biztonsági eseménykezelési terv jogosulatlanok számára ne legyen megismerhető, módosítható.

- Képzés a biztonsági események kezelésére. A szervezet kötelezettsége, hogy biztonsági eseménykezelési képzést biztosítson az elektronikus információs rendszer felhasználói számára a feladatellátásban kijelölt szerepkörükkel és felelősségeikkel összhangban. A képzést köteles a szervezet megtartani:
  - a biztonsági eseménykezelési szerepkör vagy felelősség kijelölését követő, meghatározott időtartamon belül vagy
  - az elektronikus információs rendszer változásainak függvényében vagy
  - meghatározott gyakorisággal.

Tehát a 3. biztonsági osztályba sorolt elektronikus információs rendszer esetén az eseménykezelés adminisztratív védelmi oldalról minden elemre kiterjed. Tartalmazza a szabályozási feladatokat, a fentiekben említett PreDeCo-elvhez és az Ibtv. 6. §-ában előírtakhoz igazodva az észlelési és beavatkozási pontokat (figyelés, jelentés, kezelés), valamint a képzéssel összefüggő intézkedéseket.

2.1.4.4. A 4. biztonsági osztálytól kötelező intézkedések köre

A 4. és 5. biztonsági osztályba sorolt elektronikus információs rendszerek esetében az eseménykezelés adminisztratív védelmi oldaláról a BM rendelet – az előző fejezetben ismertetett elvárások mellett – előírja az automatizált folyamatokat és a rendszerszintű szabályozást is. Ennek elemei a következők:

- Automatizált jelentés: a szervezet automatizált mechanizmusokat (például folyamattámogató alkalmazás) alkalmaz, hogy segítse a biztonsági események jelentését.
- Automatizált támogatás biztosítása: a szervezet automatizált mechanizmusokat alkalmaz, hogy növelje a biztonsági események kezelésével kapcsolatos információk és a támogatás rendelkezésre állását.
- Biztonsági események kezelésének tesztelése: a szervezet meghatározott gyakorisággal teszteli az elektronikus információs rendszerre vonatkozó biztonsági eseménykezelési képességeket, előre kidolgozott tesztek felhasználásával, annak érdekében, hogy meghatározza a biztonsági eseménykezelés hatékonyságát és dokumentálja az eredményeket.
- Egyeztetés: a szervezet egyezteti a biztonsági eseménykezelés tesztelését a kapcsolódó tervekért (például üzletmenet-folytonossági terv és katasztrófa-elhárítási terv) felelős szervezeti egységekkel.

2.1.4.5. Az 5. biztonsági osztálytól kötelező intézkedések köre

Az 5. biztonsági osztályba tartozó elektronikus rendszerek esetében az előzőekben felsorolt cselekvések mellett a szervezet köteles biztosítani a következő intézkedéseket is:

- Automatikus eseménykezelés: a szervezetnek automatizált mechanizmusokat kell alkalmaznia az eseménykezelési eljárások támogatására (például folyamattámogató alkalmazás).
- Információ korreláció: a szervezet a biztonsági eseményekre vonatkozó információkat és az egyedi eseményekre való reagálásokat összekapcsolja annak érdekében, hogy szervezetszintű rálátást nyerjen a biztonsági eseményekkel kapcsolatos tudatosságra és a reagálásokra.
- Automatikus nyomon követes, adatgyűjtés és vizsgálat: a szervezet automatizált mechanizmusokat (például figyelőrendszerek) alkalmaz annak érdekében, hogy segítse a biztonsági események nyomon követését és a biztonsági eseményekre vonatkozó információk gyűjtését, vizsgálatát.

- Biztonsági események szimulációja: a szervezet köteles a biztonsági események kezelési képzésébe szimulált eseményeket belefoglalni, annak érdekében, hogy elősegítse a személyzet hatékony reagálását a kritikus helyzetekben.
- Automatizált képzési környezet biztosítása: a szervezet automatizált mechanizmusokat alkalmaz, hogy a biztonsági események kezelési képzéséhez mélyrehatóbb és valószerűbb környezetet biztosítson.

2.1.5. A BM rendelet 4. melléklete szerinti védelmi intézkedési katalógus

A BM rendelet 4. mellékletének 3. alcíme az *Adminisztratív védelmi intézkedések* cím alatt szervezeti szintű alapfeladatként[32] írja elő az informatikai biztonsági szabályzat (a továbbiakban. IBSZ) készítését azzal, hogy annak tartalmaznia kell:

- a biztonsági helyzet- és eseményértékelés eljárási rendjét,
- a biztonsági események – ideértve az adatok sérülését is – bekövetkeztekor követendő eljárást, ideértve a helyreállításra vonatkozó rendelkezéseket is.

A katalógus a *Logikai védelmi intézkedések* fejezetben, a *Rendszer- és információsértetlenség* cím alatt szabályozza a biztonsági riasztások és tájékoztatások kezelésének rendjét a szervezetben:

- folyamatosan figyelje a kormányzati eseménykezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket,
- folyamatosan kísérje figyelemmel a Nemzeti Elektronikus Információbiztonsági Hatóságtól érkező értesítéseket,
- szükség esetén belső biztonsági riasztást és figyelmeztetést adjon ki, és azt juttassa el az érintett személyekhez,
- alakítsa ki és működtesse az események bejelentési kötelezettségének rendszerét,
- megfelelő ellenintézkedéseket és válaszlépéseket tegyen egy biztonsági esemény bekövetkezése esetén.

Ezeken túl a szervezet köteles olyan naplózási eljárásrendet is kialakítani, amely elősegíti az Ibtv. mellett az adatvédelmi jogszabályokban is egyre nagyobb jelentőséget nyerő *elszámoltathatóság elvének* történő megfelelést, azzal, hogy a naplóbejegyzésekben elegendő információ begyűjtésére kerüljön sor annak érdekében, hogy ki lehessen mutatni, milyen események történtek, miből származtak ezek az események és mi volt ezek kimenetele.

2.1.6. Az eseménykezelés nemzeti intézményrendszere

Az Ibtv. hatálya alá tartozó elektronikus információs rendszerek biztonságának felügyeletét[33] a törvény 2013-as elfogadásakor megszülető végrehajtási rendeletek még megosztották a Nemzeti Fejlesztési Minisztérium és az alá tartozó Nemzeti Elektronikus Információbiztonsági Hatóság (a továbbiakban: NEIH), illetve a Belügyminisztérium között. A jogszabálycsomag 2015-ös novelláris felülvizsgálatát követően azonban az információbiztonság teljes életciklusára vonatkozó feladatokat egységesen a Belügyminisztérium irányítása alatt működő Nemzetbiztonsági Szakszolgálat újonnan létrejövő Nemzeti Kibervédelmi Intézete (a továbbiakban NKI) örökölte.[34] Az NKI a feladatait megosztja

[32] BM rendelet, 4. melléklet 3. alcím 3.1.1. alpontja.

[33] Ibtv. 14. § (1) bekezdés.

[34] Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) kormányrendelet 2. §-a.

a kormányzati eseménykezelő központ, azaz a Számítógépes Vészhelyzeti Reagáló Egység (Computer Emergency Response Team, a továbbiakban: GovCert), illetve a NEIH között.[35]

Az eseménykezeléssel összefüggésben a NEIH a következő feladatokat látja el:

- ügyfelek és rendszerek nyilvántartása;
- a biztonsági eseményekkel kapcsolatos bejelentések kivizsgálására irányuló hatósági eljárás megindítása;
- az eseménykezelő központokkal való kapcsolattartás;
- a biztonsági eseményekkel kapcsolatos, a kormányzati eseménykezelő központtól kapott értesítések nyilvántartása és kezelése;
- javaslat tétele információbiztonsági felügyelő kirendelésére (amennyiben a szerv önállóan nem tud megbirkózni a törvényben meghatározott, az információbiztonsághoz kapcsolódó feladataival).

Az Ibtv. hatálya alá tartozó szervek a tudomásukra jutott biztonsági események adatait haladéktalanul kötelesek a GovCert részére továbbítani.[36] A GovCert feladata elsősorban a kibertér irányából érkező, valamint az Ibtv. hatálya alá tartozó szervezetek működését biztosító infokommunikációs infrastruktúra, illetve a szervek nyílt elektronikus információs rendszereit érintő biztonsági események és fenyegetések kezelése.[37] Ebbe beletartozik, hogy feladatellátása során[38]

- a nemzetközi eseménykezelési együttműködésben képviseli Magyarországot;
- a magyar kiberteret érintő nemzetközi bejelentéseket fogadja és kezeli;
- sérülékenységi vizsgálatot folytat;
- kapcsolatot tart a szervezetekkel a bejelentett biztonsági események fogadására, valamint az azok kezeléséhez szükséges intézkedések megtétele és koordinációja érdekében;
- folyamatos ügyeleti szolgálatot működtet;
- elvégezheti a biztonsági események adatainak műszaki vizsgálatát, amelyhez adatokat és az adatokhoz elektronikus hozzáférést kérhet;
- a kritikus hálózatbiztonsági fenyegetettségekről magyar nyelven azonnali figyelmeztetéseket tesz közé;
- képzéseket és tudatosító akciókat szervez;
- a biztonsági események kezelésében együttműködik a NEIH-vel, továbbá más érintett szervezetekkel;
- gyűjti a szervezeteknél előforduló biztonsági események adatait, ezekről negyedévente jelentés készít a Nemzeti Kiberbiztonsági Koordinációs Tanács[39] részére.

Az Ibtv bátorítja az adatkezelőket, hogy a biztonsági események kivizsgálását a hatóság felhívása nélkül is kezdeményezze a kormányzati eseménykezelő központnál.[40]

A személyes adatokat is érintő biztonsági események esetén, az incidensek nyilvántartási kötelezettsége kapcsán a hatályos nemzeti jogunk feladatokat és hatáskört telepít a fentieken túl még a Nemzeti Adatvédelmi és Információszabadság Hatósághoz, illetve az elektronikus hírközlési szolgáltatók esetében a Nemzeti Média- és Hírközlési Hatósághoz, ezeket később részletesen megvizsgáljuk.

---

[35] Lásd: http://nbsz.hu/?mid=42 (a letöltés ideje: 2017. április 30.)

[36] Ibtv. 19. § (1) bekezdés.

[37] Kivételt képeznek ez alól az Ibtv. 19. § (2) és (5) bekezdései alapján egyes speciális elektronikus információs rendszerek, amelyeket az úgynevezett ágazati eseménykezelő központok kezelnek:
a) a kijelölt létfontosságú rendszerelemek elektronikus információs rendszereit érintően az országos Katasztrófavédelmi Főigazgatóság,
b) a honvédelmi célú elektronikus információs rendszereket érintően a Katonai Nemzetbiztonsági Szolgálat,
c) a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereit érintően az Információs Hivatal,
amelyek a tudomásukra jutott biztonsági események adatait kötelesek haladéktalanul bejelenteni a GovCert részére.

[38] Ibtv. 20. §.

[39] Ibtv. 21. §.

[40] Ibtv. 18. § (2)–(9) bekezdései szerint, mely alól azonban kivételt képeznek a zárt célú elektronikus információs rendszerek, az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemek, valamint a nemzetbiztonsági védelem alá eső szervezetek.

2.1.7. Adatvédelem, adatbiztonság és információbiztonság

Adatvédelem alatt a magyar jogi terminológiában az 1990-es évek elejétől kezdve a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összességét értjük.[41] Tehát az adatvédelem főleg alapjogi,[42] személyiségi jogi és szabályozási szemszögből vizsgált, jogi megközelítést (is) igénylő terület.

Az információbiztonság, a biztonsági események megelőzése, kezelése kapcsán ugyanakkor jellemzően az informatikai üzemeltetés, illetve az azt felügyelő informatikai biztonságért felelős személyek szerepét, feladatait vizsgálja a szakirodalom. Ugyan az információbiztonságra vonatkozó szabványokban és ajánlásokban többnyire megjelenik a jogszabályi előírásoknak való megfelelés követelménye,[43] ám a gyakorlatban hagyományosan az információs rendszer korábban vizsgált fizikai, logikai, esetenként adminisztrációs védelmére helyeződik a hangsúly, és a jogi előírások között sem az adatvédelem az először vizsgált elem. A 41/2015. (VII. 15.) BM rendelet 1. melléklete szerinti biztonsági osztályba sorolásnál, illetve a szervezet 2. melléklet szerinti biztonsági szintje szempontjából azonban már meghatározó jelentőségű a személyes adatok vagy azok különleges típusainak kezelése, és a később részletesen bemutatandó 2016/1148 (EU) hálózatbiztonsági irányelv is utal az adatvédelmi előírásokra.

A 2018 májusáig hatályos adatvédelmi jogi előírások szintén tartalmaznak adatbiztonsági követelményeket: az adatvédelmi irányelv 17. cikkéhez hasonlóan az Infotv. 7. § (3) bekezdése értelmében a személyes adatot kezelő vagy feldolgozó[44] személy feladata az adatokat „*megfelelő intézkedésekkel védeni a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen”.* Adatbiztonság alatt az Infotv. tehát a személyes adatok információbiztonságát érti.[45]

Személyes adatok automatizált (elektronikus rendszerben történő) feldolgozása során az Infotv. tovább pontosítja az adatbiztonsági elvárásokat,[46] és még a 41/2015. (VII. 15.) BM rendelet előírásainál is szigorúbban, általános jelleggel kötelezi az adatkezelőt vagy adatfeldolgozót, hogy az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel legyen a technika mindenkori fejlettségére: *„Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek.”*[47]

Szádeczky Tamás azonban felhívja a figyelmet arra (Szádeczky 2012), hogy a hatályos jogi környezetben az adatbiztonság szabályozása kapcsán szakadék tapasztalható a jogalkotás és a jogalkalmazás (tipikusan jogászok), valamint az intézkedések végrehajtói (fejlesztők, üzemeltetők, informatikusok) között. Ennek oka, hogy a jogi (adatvédelmi) követelmények mögötti technikai tartalom nem kellően pontos, a technológiafüggetlenség és az időtállóság követelménye miatt nehezen ismerhető fel

[41] Adatvédelmi szótár, http://naih.hu/adatvedelmi-szotar.html (a letöltés ideje: 2017. április 20.)

[42] A magánszféra védelméhez, illetve a személyes adatok védelméhez fűződő jog a legtöbb tagállamban alapjogi védelmet élvez. Hazánkban ezt az Alaptörvény VI. cikke rögzti. Az Európai Unió működéséről szóló szerződés és az Európa Unió Alapjogi Chartája szintén garantálja e jogokat, erre tekintettel az unió konkrét jogalappal rendelkezik arra, hogy jogszabályokat fogadjon el ennek az alapvető jognak a védelmére, így születhetett meg a GDPR is.

[43] Lásd például az ISO/IEC 27001:2013 szabvány A. melléklet 18. pontjának *Megfelelés a jogi és szerződéses követelményeknek* címét.

[44] Az Infotv. 3. § 17. pontja értelmében adatfeldolgozás „az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adaton végzik.” Tipikusan ilyennek minősül a tárhelyszolgáltatás, a felhőalapú szolgáltatások (SaaS vagy Database-aas) nyújtása, illetve a nyomdai, kézbesítési szolgáltatások is.

[45] A NAIH adatvédelmi szótára megfogalmazása szerint: „Az adatok jogosulatlan megszerzése, módosítása és megsemmisítése elleni műszaki és szervezési megoldások rendszere.” Adatvédelmi szótár, http://naih.hu/adatvedelmi-szotar.html (a letöltés ideje: 2017. április 20.)

[46] Lásd Infotv. 7. § (5).

[47] Infotv. 7. § (6).

az elvárt védelmi intézkedés,[48] de ez a felületesség a jogalkalmazást rendkívüli módon megnehezíti (Reidenberg–Joel 1998). A jogalkotónak sokkal tájékozottabbnak kellene lennie a szabályozott technológiákat illetően (például biometrikus adatok kezelése, cloud computing, RFID), mivel az adatvédelmi jogszabályok hatálya ki kell terjedjen az adatbiztonság területére is (Európai Bizottság 2009). A technológiai megoldások alkalmazásával (például a privát szférát erősítő technológiák, álnevesítés) is erősíteni lehet az adatvédelmet, amelyek érvényre juttathatják a magánszférát védő jogi előírásokat.[49]

2.1.8. Adatvédelmi incidensek nyilvántartási és bejelentési kötelezettsége 2018-ig

Általános, minden személyes adatot kezelő szervezetre kiterjedő, az adatvédelmi incidensekre vonatkozó nyilvántartási és bejelentési, illetve értesítési kötelezettség a GDPR hatályba lépéséig nem található a magyar adatvédelmi jogban. Azonban az elektronikus hírközlési ágazatban már 2009 óta találunk ilyen előírásokat a személyes adatok biztonságának sérülése esetére.[50] Ezért a jelenlegi előírásokat is fontos áttekinteni, hogy megállapíthassuk: az új előírások mennyiben jelentenek majd változást a jelenlegi adatkezelői gyakorlathoz képest.

A GDPR 2012-től nyilvánosan elérhető szövegtervezete már elfogadása előtt komoly hatást gyakorolt a tagállamok adatvédelmi jogára. Az új szabályokra történő átállás megkönnyítése érdekében a magyar jogalkotó 2015 őszén törvénybe iktatta az adatvédelmi incidens fogalmát, valamint előírta a kapcsolódó nyilvántartási és a kérelemre történő tájékoztatási kötelezettséget. Az Infotv. 3. § 26. pontja a *„személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés”* eseteit minősíti adatvédelmi incidensnek, mely fogalom értelmezésére még visszatérünk a későbbiekben.

A törvény rögzíti, hogy amennyiben az érintett tájékoztatást kér személyes adatai kezeléséről, akkor az adatkezelő köteles őt tájékoztatni az adatait esetlegesen érintő adatvédelmi incidens(ek) bekövetkezéséről, annak körülményeiről, hatásairól és az elhárítására megtett intézkedésekről is.[51] A NAIH számára megkeresés esetén ugyanezekről az adatokról kell tájékoztatást adni, az adatkezelőnek külön bejelentési kötelezettsége nincs. Előbbiek mellett az adatkezelő nyilvántartást kell vezessen a bekövetkezett incidensekről *„az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából”,* amelyben rögzíti az érintett személyes adatok körét, az incidenssel érintettek körét és számát, az esemény időpontját, körülményeit, hatásait és az elhárítására megtett (adatbiztonsági) intézkedéseket.[52] Tehát a nyilvántartásban nem rögzítheti az incidensben érintett konkrét személyek adatait, csak a személyi kört, mivel az már az adatok kezelésének eredeti célját, időtartamát meghaladná, ezért a gyakorlatban nehezen teljesíthetőnek tűnik az elvárás, hogy az adatkezelő az érintettek kérésére képes legyen tájékoztatást adni az ő adatait érintő incidensről. Azonban a GDPR alkalmazhatóságáig az adatkezelő nem köteles sem a nemzeti felügyelő hatóságnak (NAIH) bejelentést tenni, sem az érintetteket értesíteni az adatvédelmi incidens bekövetkeztéről.

---

[48] „Az informatikai biztonság szabályozottsága tekintetében az adatvédelmet felületesen szabályozott területnek tekinthetjük, ugyanis a jogi szabályok előírásra kerültek, de azokat a jogalkotó nem részletezte, ebből kifolyólag a jogalkalmazó és a betartásra kötelezett nehezen tudja értelmezni azokat, az önkéntes jogkövetés így nagymértékben megnehezül.” (Szádeczky 2013, 153.)

[49] A privát szférát erősítő technológiák (PETs) az egyén identitását, személyazonosságát védő technikai és szervezeti megoldások gyűjtőneve. Alkalmazásuk alapvető célja, hogy ne csak az adatokat általában, hanem az adatalanyokat, az érintetteket is védjék a visszaélések ellen, és elősegítsék az információs önrendelkezéshez való jog érvényesítését a technológiai megoldásokat felhasználva. (Kiss 2013, 113.)

[50] Az Európai Parlament és a Tanács az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK (2002. július 12.) irányelvébe (a továbbiakban: EU elektronikus hírközlési adatvédelmi irányelv) rendelkezései közé a 2009/136/EK irányelv ültette át a kötelezettséget.

[51] Infotv. 15. § (1).

[52] Infotv. 15. § (1a).

Az elektronikus hírközlésről szóló 2003. évi C. törvény (a továbbiakban: Eht.) ültette át a hazai jogrendbe a 2002/58/EK irányelv incidensekre vonatkozó előírásait,[53] amely már rendelkezik a fenti két kötelezettségről is, igaz, csak az adatkezelők egy jóval szűkebb körére, a hírközlési szolgáltatók adatkezelésére nézve. A törvény szerint: az *„előfizetői személyes adatok megsértését jelenti a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtásával összefüggésben továbbított, tárolt, vagy más egyéb módon kezelt vagy feldolgozott személyes adatok véletlen, vagy jogellenes kezelése vagy feldolgozása, így különösen megsemmisítése, elvesztése, módosítása, jogosulatlan felfedése, nyilvánosságra hozatala, vagy az azokhoz való jogosulatlan hozzáférés”*.[54]

Az Eht. hatálya alá eső magyar hírközlési szolgáltatók a „személyes adatok megsértése” esetén kötelesek haladéktalanul,[55] de legkésőbb 24 órán belül[56] bejelentést tenni az illetékes hatóságnak.[57] Amennyiben az esemény várhatóan hátrányosan érinti az előfizető vagy más magánszemély személyes adatait vagy magánéletét, akkor erről az előfizetőt vagy magánszemélyt is indokolatlan késedelem nélkül értesítenie kell. E kötelezettség alól a GDPR előírásaihoz[58] hasonlóan csak akkor mentesülhet a szolgáltató, ha igazolni tudja, hogy végrehajtotta a megfelelő technikai védelmi intézkedéseket (például technológiai titkosítás), illetve hogy ezen intézkedéseket alkalmazták is az incidenssel érintett adatoknál, és ezzel értelmezhetetlenné teszik azokat az adatokhoz jogosulatlanul hozzáférő számára.[59]

A szolgáltató emellett az Infotv. nyilvántartási előírásához képest speciális, azt helyettesítő incidens-nyilvántartást köteles vezetni annak érdekében, hogy az NMHH ellenőrizni tudja, a szolgáltató megfelelően értesítette-e az érintetteket vagy az értesítés mellőzése esetén helyesen mérlegelte-e az incidens következményeit, illetve alkalmazta a technikai és védelmi intézkedéseket.[60]

Ahogy azt Szőke Gergely László is kifejti (Szőke 2017), az EU elektronikus hírközlési adatvédelmi irányelvének szóhasználata nem azonos az előírásokat a magyar jogba átültető Eht. fenti fogalommeghatározásával. Az Eht. *„személyes adatok véletlen, vagy jogellenes kezelése vagy feldolgozása”* fordulata nem szerepel az irányelvben, és az jóval tágabb esetkört fed le a biztonsági incidens európai jogalkotó által rögzített fogalmánál. Személyes adatok jogellenes, tehát az Infotv. előírásaiba ütköző kezelése ugyanis megvalósulhat a céltól eltérő vagy nem megfelelően meghatározott jogalappal történő adatkezeléssel, esetleg az adatkezeléshez kapcsolódó előzetes tájékoztatási kötelezettség elmulasztásával is, amely esetekben azonban nem beszélhetünk az adatok biztonságának sérüléséről. Az Infotv. korábban ismertetett meghatározása szintén a vitatott „*személyes adat jogellenes kezelése vagy feldolgozása*” fordulat átvételével született meg, amely így szintén az esetek jóval szélesebb körét minősíti adatvédelmi incidensnek, mint amit az információbiztonság területén elterjedt *biztonsági esemény* fogalma lefedne, illetve amit a GDPR meghatározása nyilvántartani (bejelenteni) rendel. Az EU elektronikus hírközlési adatvédelmi irányelvét értelmező, a 29. cikk szerinti Adatvédelmi Munkacsoport által kiadott vélemény (29. cikk szerinti Adatvédelmi Munkacsoport 2014) szintén arra utal, hogy az adatvédelmi incidens az információbiztonság klasszikus hármas követelményeinek, a „bizalmasság, sértetlenség, rendelkezésre állás” megsértését jelenti, tehát 2018 májusától a kapcsolódó hazai gyakorlatot is ennek megfelelően szükséges változtatni.

---

[53] EU elektronikus hírközlési adatvédelmi irányelv, 2. cikk i) pont: „A biztonság olyan megsértése, amely a Közösségben nyilvánosan elérhető hírközlési szolgáltatások nyújtásával összefüggésben továbbított, tárolt vagy más módon feldolgozott személyes adatok véletlen vagy jogellenes megsemmisítését, elveszítését, módosítását, jogosulatlan felfedését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.” Az angol ’data breach’ kifejezést a hazai jogban a ’személyes adatok megsértése’ terminológiával vették át.

[54] Eht. 156. § (2).

[55] Az Eht. 156. §-a előírásai szerint.

[56] 611/2013/EU Bizottsági rendelet 2. cikk (2), valamint 4/2012. (I. 24.) NMHH Rendelet 5. § (2) alapján.

[57] 2002/58/EK, 4. cikk (3). Hazánkban az Eht. 156. § (3) alapján ezt a Nemzeti Média- és Hírközlési Hatóságnak (a továbbiakban: NMHH) kell bejelenteni.

[58] GDPR 34. cikk (3) bekezdés a) pontja.

[59] 2002/58/EK, 4. cikk (3), illetve az azt átültető Eht. 156. § (5) bekezdése.

[60] Eht. 156. § (4) bekezdés.

2.1.9. Az Európai Digitális Menetrend 2014–2020 céljai

A 2008-ban kirobbant pénzügyi és gazdasági világválság, a számítógépes bűncselekmények számának növekedése, illetve a kiberhadviselés és kémkedés megjelenése új kihívások elé állította az Európai Uniót. Nyilvánvalóvá vált, hogy az előttünk álló időszak erőteljes modernizációból és globalizációból eredő kihívásait csak a digitális belső piacra vonatkozó, hosszú távú stratégiai tervdokumentumok megalkotásával lehet hatékonyan kezelni. Így született meg a 2020-ig tartó időszak intézkedéseinek alapdokumentumaként az *Európa 2020 foglalkoztatási és növekedési stratégia* (a továbbiakban: Európa 2020).[61]

Az *Európa 2020* keretében az Európai Bizottság hét kiemelt szabályozási területet azonosított, köztük az intelligens növekedés célrendszerén belül az *Európai Digitális Menetrend 2014–2020 stratégiát* (a továbbiakban: Digitális Menetrend). A dokumentum célja, hogy a digitális technológia előnyei az európai polgárok és vállalkozások számára minél szélesebb körben elérhetőek legyenek. Kiemelt feladatként nevesíti ehhez az uniós adatvédelmi szabályozás felülvizsgálatát, a távközlési szolgáltatások egységesítését, a digitális tér és elektronikus szolgáltatások iránti bizalom és az internetes biztonság megerősítését, valamint a szükséges IT-infrastruktúra és a lakosság digitális jártasságának, digitális készségeinek fejlesztését.

A Digitális Menetrend *Bizalom és biztonság* című intézkedési területén az Európai Bizottság számára megjelenő alábbi feladatok vezettek végül a GDPR és a NIS irányelv elfogadásához:

- Javaslattétel az információs rendszerek elleni számítógépes támadások leküzdésére irányuló szigorúbb jogszabályokra, illetve a számítógépes bűnözésre vonatkozó joghatósággal kapcsolatos európai és nemzetközi szintű szabályokra.
- Számítógépes támadások elleni, gyors reagálású európai rendszer és ennek részeként a számítógépes szükséghelyzeteket kezelő csoportok (CERT) hálózatának létrehozása, az európai hálózat- és információbiztonsági ügynökség (ENISA) szerepének megerősítése.
- Javaslattétel olyan tagállami forróvonalak létrehozására, ahol a gyermekek és szüleik bejelentést tehetnek a jogellenes internetes tartalmakról.
- Tudatosságnövelés, így többek között az internetes védelem iskolai oktatása.
- Egyebek mellett a gyermekbántalmazással, a személyazonosság-lopással és a számítógépes bűnözéssel kapcsolatos válaszmechanizmusok kidolgozása.
- A magánélethez és a személyes adatok védelméhez való jog általános érvényesítése a digitális és való világban is.

2.1.10. Eseménykezelési elvárások a GDPR szabályozásában

2.1.10.1. A GDPR viszonya a hatályos adatvédelmi előírásokhoz

2018. május 25-től valamennyi tagállamban egységesen és közvetlenül alkalmazandó az EU Általános Adatvédelmi Rendelete, bevett rövidítése alapján a GDPR. A jogszabály a több mint húsz éve hatályban lévő 95/46/EK irányelvet[62] (a továbbiakban: Adatvédelmi irányelv) váltja fel, és közvetlen alkalmazhatósága miatt az irányelv rendelkezéseit átültető tagállami adatvédelmi jogszabályok, köztük az Infotv. GDPR-ban már szabályozott tárgyköreinek[63] is a helyébe lép.

---

[61] A 2010-ben elfogadott dokumentum célja, hogy megteremtse az intelligens (hatékonyabb oktatási, kutatási és innovációs beruházások, valamint a digitális társadalom fejlesztése), fenntartható (erőforrás-hatékonyabb, környezetbarát és versenyképes gazdaság) és inkluzív (a gazdasági, szociális és területi kohéziót előmozdító, magas foglalkoztatási arányt biztosító) növekedés feltételeit.

[62] Az Európai Parlament és a Tanács a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelve (1995. október 24.).

[63] A közérdekű és közérdekből nyilvános adatokra vonatkozó szabályokat, valamint egyes, a GDPR által nem rendezett adatvédelmi előírásokat azonban továbbra is a nemzeti jogban, tehát az Infotv.-ben rögzítik; például a Nemzeti Adatvédelmi és Információszabadság Hatósággal (a továbbiakban: NAIH) kapcsoltos szakaszok nem változnak.

Az internet korának hajnalán elfogadott Adatvédelmi irányelv a személyes adatok kezelésének legfontosabb elveit, köztük az adatkezelés biztonságára vonatkozó szabályokat[64] is sikerrel ültette át a tagállami jogokba Európa-szerte, de az egyes országok jogalkotása és jogalkalmazása közötti eltérések széttagolttá tették az európai adatpiacot (Európai Bizottság 2015). A reform egyik kiemelt célja ezért az volt, hogy a személyes adatok védelme és az információbiztonsági követelmények egységesen magas szintje mint egymást kölcsönösen feltételező és kiegészítő garanciák segítségével növekedjen a felhasználók új technológiákba és az online térbe vetett bizalma, ezáltal felgyorsuljon az egységes európai digitális szabályozás létrejötte (Európai Bizottság 2010).

A GDPR a személyes adatokat kezelő szervezetek számára az elődjénél sokkal részletesebb adatbiztonsági előírásokat tartalmaz: a megfelelőség bizonyítását széles körű és részletes dokumentációhoz köti,[65] illetve már az adatok kezelésének megkezdése előtt kockázatalapú[66] tervezést, az adatvédelmi garanciák számbavételét[67] várja el. Komoly figyelmet fordít az adatkezelési műveletekhez kapcsolódó technológiákra (titkosítás, álnevesítés), és rögzíti, hogy minden adatkezelő köteles dokumentálni, bizonyos esetekben bejelenteni, valamint az érintetteket is tájékoztatni a személyes adatokat érintő incidensekről.

A GDPR új előírásai között megjelenik a *beépített és alapértelmezett adatvédelem* elve.[68] A kanadai „Privacy by Design" filozófiájának európai jogba ültetését megkísérlő rendelkezés értelmében az érintett magánszférájának védelmét és az adatvédelmi szabályozás elveit integrálni kell a különböző adatkezelő technológiák követelményrendszerébe, amely így a számítástechnikai és üzleti alkalmazások integráns részévé válik anélkül, hogy azok funkcionalitást korlátozná. Az elméletet kialakító volt adatvédelmi biztos elismeri a biztonság jelentőségét, de úgy kíván eredményeket elérni, hogy közben nem sérti szükségtelenül az érintettek széles körének magánszféráját, kölcsönös előnyökre törekszik (Cavoukian 2016). Az elv gyakorlati megvalósulásának egyik legfontosabb eleme a Székely Iván (Székely 2008) által *privát szférát erősítő technológiáknak* fordított „Privacy Enhancing Technologies", azaz PETs-ek fejlesztése, alkalmazása és azok terjedésének elősegítése.

2.1.10.2. A GDPR adatbiztonsági rendelkezései és incidenskezelésre vonatkozó előírásai

A GDPR számos újdonságot hoz – az adatbiztonság területén is – az Adatvédelmi irányelv és az Infotv. előírásaihoz képest, ezért a jogalkotó a szabályoknak történő megfelelésre két év felkészülési időt adott. Az adatbiztonság 2018. májusig hatályos általános megfogalmazását[69] kiegészíti a kockázatok értékelésével és a védekezés költségeinek mérlegelésével: *„A tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy*

[64] Az Adatvédelmi irányelv 17. cikke rendelkezik az adatbiztonsági előírásokról, azonban az adatbiztonság megsértésének kezelésére nem ír elő kötelezettséget az adatkezelőnek.

[65] Ki kell emelnünk a GDPR 35. cikkében rögzített adatvédelmi hatásvizsgálat készítésére vonatkozó kötelezettséget, melynek lefolytatását az adatkezelő és az adatfeldoglozó az elszámoltathatóság érdekében a 29. cikk szerinti Adatvédelmi Munkacsoport WP 248. számú, adatvédelmi hatásvizsgálatról szóló iránymutatása alapján részletesen dokumentálni köteles, illetve eredményét legalább részben közzé is kell, hogy tegye az érintettek számára (29. cikk szerinti Adatvédelmi Munkacsoport, 2017).

[66] A GDPR 32. cikkének megfogalmazása szerint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével kell kialakítani az adatbiztonsági intézkedéseket.

[67] A GDPR 25. cikke írja elő a beépített és alapértelmezett adatvédelem elvének alkalmazását is, amely alapján adatkezelő „a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket – például álnevesítést – hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt az e rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába."

[68] GDPR 25. cikk

[69] Adatvédelmi irányelv, 17. cikk.

a kockázat mértékének megfelelő szintű adatbiztonságot garantálja." A GDPR emellett példálózó felsorolást is ad az elvárt védelmi intézkedésekről. Ahol szükséges és lehetséges, ott

- alkalmazni kell a személyes adatok álnevesített,[70] azaz pszeudonim kezelését, technológiai titkosítását;
- az adatkezelőnek vagy feldolgozónak biztosítania kell, hogy a személyes adatok kezelésére használt rendszerekben és szolgáltatásokban folyamatos védelmi intézkedések működjenek;
- fizikai vagy műszaki incidens esetén rendelkezésre áljon biztonsági mentés vagy tartalék rendszer;[71]
- az adatkezelő a védelmi intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást alakítson ki.[72]

A GDPR meghatározza emellett az adatvédelmi incidens fogalmát: *„A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi*."[73] Tehát az információbiztonsági eseményeknek csak azon típusait értjük alatta, amelyek a személyes adatok biztonságát sértik.

A fenti meghatározásból az következik, hogy minden olyan esemény, amely akár csak egyetlen természetes személy adatát érinti, már adatvédelmi incidensnek minősül, még akkor is, ha annak minimális az érintett magánszférájára gyakorolt hatása. Tehát a fogalom kapcsán többnyire nem a médiában is hírértékkel bíró, komoly károkat okozó adatvesztésekre kell elsősorban gondolni, hanem a hétköznapi adatkezelési tevékenységek során felmerülő, emberi vagy technikai hibákra, téves adatkezelési műveletekre (például egy rossz címzettnek elküldött, személyes adatokat tartalmazó e-mailre).

A rendelet preambuluma kifejti, hogy az adatvédelmi incidens megfelelő és jól időzített védelmi intézkedések hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat az adatalanyoknak.[74] Ha egyes biztonsági incidensek, veszélyek *„valószínűsíthetően magas kockázatot"* jelentenek a természetes személyek jogaira és szabadságaira – tehát nem az adatkezelő személy vagy szervezet érdekeire – nézve, akkor arról az érintetteket is értesíteni kell. Ennek célja, hogy az értesítés hatására az érintett olyan intézkedéseket tehessen adatai védelmében – például jelszavának megváltoztatása annak kompromittálódása esetén vagy bankkártyája letiltatása –, amelyekkel csökkentheti az incidens által okozott károkat.[75] Szőke Gergely László szerint (Szőke 2017) az adatvédelmi incidensek bejelentési kötelezettségének lényege az, hogy:

- ez alapján a nemzeti adatvédelmi hatóság meg tudja tenni a szükséges intézkedéseket, és a bejelentések tartalmából akár egyes adatkezelői csoportokra, szolgáltatási területekre nézve is adatot szerezhet az adatbiztonság tényleges helyzetére vonatkozóan;
- az adatkezelő a személyes adatokat ért incidenseket felismerje, körülményeit felderítse, azokat megfelelően dokumentálja, ami aztán kijelöli a védelmi intézkedések fejlesztésének irányait;
- valamint az adatkezelő a jó hírnevét is veszélyeztető incidensek és a hozzájuk kapcsolódó értesítési kötelezettségek előfordulásának minimalizálása érdekében jelentős erőforrásokat fordítson

[70] A GDPR 4. cikk 5. pontja meghatározása szerint az álnevesítés „a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni."

[71] A GDPR 32. cikk (1) c) pontja megfogalmazásában: „Az arra való képesség, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani."

[72] GDPR 32. cikk (1) a)–d).

[73] GDPR 4. cikk 12. pont.

[74] A GDPR Preambulum (85) ide sorolja „a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, az álnevesítés engedély nélküli feloldását, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt."

[75] GDPR Preambulum (86).

az adatbiztonság szintjének növelésére, az incidenssel érintettek számának vagy a potenciális károknak a csökkentésére.

A GDPR 33. cikke ezért előírja, hogy az adatvédelmi incidens bekövetkezését az adatkezelő indokolatlan késedelem nélkül – ha lehetséges, legkésőbb 72 órával az után, hogy az a tudomására jutott – köteles bejelenteni az illetékes felügyelő hatóságnak.[76] A bejelentés legfontosabb tartalmi elemei:

- az adatvédelmi incidens jellege (körülményei) és, ha ez lehetséges, az arra vonatkozó adatok (érintettek köre és száma, az incidenssel érintett adatok köre);
- az adatvédelmi tisztviselő vagy kapcsolattartó személy neve és elérhetőségei;
- az incidens várható hatása, következményei;
- az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések.[77]

Amennyiben az adatkezelő a határidőt elmulasztja, akkor a bejelentéséhez mellékelni köteles a késedelem igazolására szolgáló indokokat is. Nem kell bejelentenie a hatóságnak az incidenst, ha az *„valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve”*.[78]

Azonban ha az adatvédelmi incidens *valószínűsíthetően magas kockázattal jár* a természetes személyek jogaira és szabadságaira nézve, az adatkezelő az érintetteket indokolatlan késedelem nélkül tájékoztatja az adatvédelmi incidensről,[79] kivéve, ha korábban mások számára értelmezhetetlenné tette az incidenssel érintett adatokat vagy az incidenst követően olyan további intézkedéseket tett, amelyekkel a kockázatokat érdemben csökkentette.[80] Az adatfeldolgozónak szintén kötelezettsége az adatvédelmi incidensek felismerése és jelzése, azonban számára még a 72 órás időtartam sem áll rendelkezésére a GDPR kapcsolódó bekezdése alapján: köteles indokolatlan késedelem nélkül tájékoztatást adni az eseményről az adatkezelő részére, hogy az meg tudja tenni az előírt lépéseket.[81]

A GDPR kötelezi az adatkezelőt, hogy nyilvántartsa az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket annak érdekében, hogy a felügyeleti hatóság ellenőrizhesse a bejelentési követelményeknek való megfelelést.[82] Tehát a nyilvántartási kötelezettség minden, a kevésbé jelentős incidensekre is kiterjed, és az elszámoltathatóság elve[83] alapján az adatkezelő az, aki köteles lesz igazolni az incidensek bejelentéséről vagy az érintett tájékoztatásának szükségességéről hozott döntését. A felügyeleti hatóság a nyilvántartást áttekintve ellenőrizheti, hogy az adatkezelő helyesen mérlegelte-e az incidens kockázatát.[84]

A fenti rendelkezéseknek különösen nagy súlyt ad, hogy azok megsértése esetén az eljáró adatvédelmi hatóság az adatkezelőt vagy feldolgozót 10 millió euróig terjedő összegű közigazgatási bírsággal vagy vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2%-át kitevő összeggel sújthatja; a két összeg közül mindig a magasabbat kell kiszabni.[85]

2.1.10.3. Gyakorlati kérdések és aggályok a GDPR előírásainak alkalmazhatósága kapcsán

A GDPR általános (magas kockázatot nem jelentő eseményekre is kiterjedő) nyilvántartási kötelezettséget ír elő valamennyi adatvédelmi incidensre és – tevékenységtől vagy szektortól függetlenül –

[76] GDPR 33. cikk (1).
[77] GDPR 33. cikk (3).
[78] GDPR 33. cikk (1).
[79] GDPR 34. cikk (1).
[80] GDPR 34. cikk (3).
[81] GDPR 33. cikk (2).
[82] GDPR 33. cikk (5).
[83] GDPR Preambulum (85), valamint 5. cikk (2) bekezdése szerint.
[84] GDPR 33. cikk (5) és 34. cikk (1).
[85] GDPR 83. cikk (4) a) pontja alapján.

valamennyi adatkezelőre nézve. A GDPR alapján az adatkezelő számára biztosított, az incidens bejelentésére nyitva álló, a tudomásszerzéstől számított legfeljebb 72 órás határidő meglehetősen rövidnek tűnhet, de a gyors reagálás a bejelentés korábban kifejtett céljait tekintve indokoltnak tűnik. A tudomásszerzés pontos időpontja nehezen bizonyítható, és az adatbiztonsági incidensek egy jelentős része hosszabb ideig vagy akár örökre rejtve marad, ami sokat gyengíthet a határidő jelentőségén, így nagyobb teret ad a jogalkalmazó adatvédelmi hatóság mérlegelésének is.

A fentiek alapján azonban az adatkezelőknek és az adatfeldolgozónak úgy kell megterveznie és kialakítania az adatkezelési rendszerét és üzleti folyamatait, hogy egy incidenst képes legyen felismerni, azokat aztán nyilvántartásba venni, majd mérlegelni az abból az érintettre vonatkozó várható kockázat mértékét, így még határidőben eleget tehessen az esetleges bejelentési és értesítési kötelezettségének. Ehhez a szervezet belső szabályaiban az incidensek észlelésére és nyilvántartására vonatkozó felelősségi szabályokat, valamint a munkatársak feladatait pontosan rögzíteni kell, valamint célszerű továbbképzések, figyelemfelhívó üzenetek útján is tájékoztatni a dolgozókat az adatvédelmi elvekről és alapfogalmakról, hogy képesek legyenek az esetleges adatvédelmi incidensek azonosítására. Az érintettek értesítésére vonatkozó kötelezettségek miatt a szervezeteknek szélesebb körben válhat indokolttá technikai titkosítást és álnevesítést alkalmaznia a személyes adatokat tartalmazó adatbázisaikban, mivel azok jelentős könnyítést eredményezhetnek a GDPR értesítési kötelezettsége alóli mentesülés miatt.

Kérdéses azonban, hogy az élet minden területén megjelenő, a személyes adatkezelésekhez kapcsolódó incidensek felismerésére, nyilvántartására és végső soron megelőzésére az új jogintézmény által sikerrel kötelezhetőek-e a fő tevékenységük szerint nem elsősorban adatkezeléssel foglalkozó kis- és középvállalkozások,[86] esetleg iskolák vagy épp az asztalfoglalást felvevő éttermek. Szintén probléma lehet, hogy az érintettek tájékoztatási kötelezettsége miatt a túl gyakran érkező értesítések összességében csökkentik majd az érintettek adatvédelmi tudatossági szintjét (Sławomir Górniak et al. 2011), és már akkor sem tesznek intézkedéseket az incidensek esetén, ha az adott esetben ténylegesen indokolt lenne.[87] Kérdéseket vet fel az is, hogyan vonható majd felelősségre az az adatkezelő, aki egy általános szerződési feltételeket alkalmazó nemzetközi adatfeldolgozó, például felhőalapú levelező szolgáltató adatszivárgásáról csak a médiából értesül majd, és honnan szerzi meg a bejelentéshez vagy értesítéshez szükséges, az incidensre vonatkozó adatokat.

A GDPR 70. cikk g) és h) pontja alapján az Európai Adatvédelmi Testület, illetve a nemzeti adatvédelmi hatóságok iránymutatásokat, ajánlásokat bocsáthatnak ki a rendeletben nem szabályozott kérdések értelmezésére, alkalmazására, így feltehető, hogy a jogintézményt további előírásokkal pontosítják 2018 tavaszáig.

A szabályozás nyertesei azonban egyértelműen a hírközlési szolgáltatók lesznek, amelyek várhatóan a hatályos jogban rögzített 24 órás határidő helyett 2018-tól csak a GDPR-ban rögzített 72 órát lesznek kötelesek tartani a bejelentések során.

2.1.11. Eseménykezelés a NIS irányelv alapján

2.1.11.1. Út az irányelv megszületéséig

Sokáig vitatott kérdésként merült fel kiberbiztonsági, informatikai szakértők körében, hogy szükséges-e az információbiztonsági elvárásokat jogszabályban is rögzíteni azok érvényre juttatása céljából, vagy a *soft law* megoldások, esetleg a szervezetek szélesebb körére értelmezhető nemzetközi iparági szabványok alkalmazása is megfelelő védelmet nyújthat az elektronikus hírközlő rendszerek számára (Szádeczky 2013).

---

[86] Hasonló aggályokat fogalmaz meg a kötelezettség általános kiterjesztésével szemben: Górniak, Sławomir et al. 2011, 6.

[87] Szőke Gergely László szerint azonban az incidensről szóló értesítés valószínűsíthetően magas kockázathoz kötése, valamint az érintett értesítése alóli kivételeknek köszönhetően ez a jelenség várhatóan elkerülhető (Szőke 2017).

A 2000-es évekig a kiberbiztonság szinte csak büntetőjogi vetülete miatt merült fel az EU döntéshozóinak programjában. Elsőként 2009-ben fogadtak el állásfoglalást a hálózat- és információbiztonság együttműködésre építő európai megközelítéséről. Az európai információs hálózatok jelenlegi egymásra utaltsága miatt azok működési problémái, adott esetben a szolgáltatások kiesései nemcsak az egyes tagállamokra lehetnek kihatással, hanem az esemény és az adott rendszer jellegétől (kritikus infrastruktúra vagy sem) függően több tagállamot is hátrányosan érhetnek – akár kihathatnak az egész Európai Unióra is.

A korábban vizsgált *Európa 2020* stratégia keretében születhetett meg az Európai Parlament, a Tanács, az Európai Gazdasági és Szociális Bizottság és a Régiók Bizottsága által jegyzett, *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér* című, az uniós stratégiáról szóló, 2013-ban közzétett közös közlemény. Ez vállalkozott először a témakör átfogó áttekintésére, a kölcsönös bizalmon alapuló, tagállami szintű együttműködés helyett a közös stratégia kialakítására. A kiberbiztonsági stratégia az alábbi kihívásokat azonosítja:

- az információs rendszerek kibertámadásokkal szembeni ellenálló képességének megteremtése;
- a kiberbűnözés drasztikus visszaszorítása;
- kibervédelmi politika kidolgozása és a közös biztonság- és védelempolitikát érintő képességek fejlesztése;
- a kiberbiztonsághoz szükséges ipari és technológiai erőforrások előteremtése;
- az Európai Unió által képviselt, a kibertérre vonatkozó egységes, nemzetközi szakpolitika kidolgozása, valamint az alapvető uniós értékek terjesztése.

Az uniós stratégia egyik fő eredménye az Európai Parlament és a Tanács a hálózati és információs rendszereknek az egész unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016/1148 irányelvének (2016. július 19.; a továbbiakban: NIS irányelv) kidolgozása és elfogadása. Ezt a jogszabályt részletesebben is bemutatjuk.

2.1.11.2. A NIS irányelv

A NIS irányelv kitér arra, hogy a fenyegetettségek egyre összetettebbek, a biztonsági események nagyságrendje, gyakorisága és hatása folyamatosan növekszik, amelyek komoly kockázatot jelentenek a hálózati és az információs rendszerek működésére nézve. A működés akadályozására vagy megszakítására irányuló szándékos és célzott cselekmények, ha azokból biztonsági esemény keletkezik, hátrányos hatást gyakorolnak az Európai Unió gazdaságára, jelentős pénzügyi veszteségeket, a felhasználói bizalom elvesztését és súlyos károkat okozhatnak.

A biztonsági események megelőzésére, kezelésére az unió országai eltérő módon vannak felkészülve. Az irányelv célja ezért az, hogy minden tagállamban kialakuljon az elégséges védekezési képesség a kibertérből érkező fenyegetettségekkel szemben, ezáltal kialakuljon a hálózati és információs rendszerek biztonságának általános uniós szintje, amely egyenlő versenyfeltételeket biztosíthat a tagállamoknak. Ehhez az szükséges, hogy a tagállamok:

- kidolgozzák saját, nemzeti szintű kiberbiztonsági stratégiájukat;
- elektronikus információbiztonságért felelős hatóságot jelöljenek ki, amely nemzeti szinten ellenőrzi a NIS irányelvben foglaltak végrehajtását;
- kijelöljenek egy vagy több (akár szektoronként különböző) biztonsági eseménykezelő csoportot (CSIRT-et);
- azonosítsák és jelöljék ki a NIS hatálya alá tartozó adatkezelőket (Magyarországon ez a Kormányzati Eseménykezelő Központ lett, 2016-ban).

A NIS irányelv 2016. augusztus 8-án lépett hatályba, a fenti célok megvalósítása érdekében valamennyi tagállamot kötelezi rendelkezéseinek 2018. május 9-ig történő átültetésére. Mivel a jogszabályt

irányelvként fogadták el, így a tagállami jogalkotók szabadon dönthetnek arról, hogy milyen módszerek és eszközök alkalmazásával érvényesítik előírásait a nemzeti jogukban.

Az irányelv hatálya az alapvető szolgáltatásokat nyújtó szereplőkre és azon digitális szolgáltatókra terjed ki, amelyeknek szolgáltatásait az alapvető szolgáltatók is igénybe veszik, ezáltal biztonságos, folyamatos és megbízható működésük nélkülözhetetlen.

Alapvető szolgáltatásokat nyújtó szereplőnek kell tekinteni azt az energiaszolgáltatás, közlekedés, banki szolgáltatások, pénzügyi piaci infrastruktúrák, egészségügy, ivóvízellátás és ivóvízelosztás, valamint digitális infrastruktúra ágazatában működő – tagállami szinten kijelölt – közjogi vagy magánjogi szervezetet, amely megfelel az alábbi kritériumoknak:[88]

- a szervezet a kritikus társadalmi és/vagy gazdasági tevékenységek fenntartásához alapvető szolgáltatást nyújt;
- az adott szolgáltatás nyújtása hálózati és információs rendszerektől függ és
- az említett szolgáltatást érintő biztonsági esemény jelentős zavart okozna a szolgáltatás nyújtásában.

Az Ibtv. hatályától eltérően a NIS irányelv csak az alapvető szolgáltatásokat nyújtó szereplőként azonosított közigazgatási szervekre alkalmazandó, az ez alá nem tartozó közigazgatási szervek hálózati és információs rendszereinek biztonságáról a tagállamoknak kell gondoskodniuk.

Digitális szolgáltatónak minősül a NIS irányelv szempontjából minden digitális szolgáltatást nyújtó szereplő. Digitális szolgáltatásnak tekinti az irányelv az online piacteret, az online keresőprogramot és a felhőalapú számítástechnikai szolgáltatást is.[89]

Nem terjed ki a NIS irányelv hatálya

- a mikro- és kisvállalatokra,
- más EU szintű, az IT-biztonságot érintő ágazati szabályozás hatálya alá (is) tartozó szereplőkre (például kritikus infrastruktúra),
- a nemzeti ágazati kijelölési kritériumokat nem teljesítő, alapvető szolgáltatást nyújtó szereplőkre,
- a hardvergyártókra és a szoftverfejlesztőkre.

2.1.11.3. Eseménykezelés és bejelentési kötelezettség a NIS alapján

Az egységes szabályozás és a gyakorlati végrehajtás támogatása érdekében a NIS irányelv meghatározza a *biztonsági esemény* és a *kockázat* fogalmát. Eszerint biztonsági eseménynek kell tekinteni minden olyan eseményt, amely ténylegesen kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára.[90] A NIS irányelv szerint minden olyan észszerűen azonosítható körülményt vagy eseményt, amely kedvezőtlen hatást gyakorolhat a hálózati és információs rendszerek biztonságára, kockázatnak kell tekinteni. [91] Minden észszerűen számításba vehető kockázatra és biztonsági eseményre kiterjedő szabályozás érdekében a NIS irányelv hatálya kiterjed az alapvető szolgáltatásokat nyújtó szereplőkre és a digitális szolgáltatókra.

A NIS irányelv védett jogi tárgya az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók hálózati és információs rendszere,[92] amely:

a) a 2002/21/EK irányelv[93] 2. cikkének a) pontja szerinti elektronikus hírközlő hálózat,

---

[88] NIS 4. cikk 4 pont, 5. cikk 2. pont.
[89] NIS 4. cikk, 6. pont, III. melléklet.
[90] NIS irányelv 4. cikk, 7 pont.
[91] NIS irányelv 4. cikk, 9. pont.
[92] NIS 4. cikk, 1. pont.
[93] Európai Parlament és a Tanács 2002/21/EK irányelve (2002. március 7.) az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról.

b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi vagy
c) az általuk működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

Hálózati és információs rendszerek biztonsága alatt a NIS irányelv a hálózati és információs rendszer arra való képességét tekinti, hogy adott bizonyossággal ellenálljon az olyan cselekményeknek, amelyek veszélyeztetik a rajtuk tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszeren nyújtott vagy rajta keresztül elérhető, kapcsolódó szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét és bizalmasságát.[94] Az alapvető szolgáltatásokat nyújtó szereplőknek és a digitális szolgáltatóknak, továbbá a tagállami és uniós szereplőknek egyaránt meg kell hozniuk minden olyan védelmi intézkedést, amelyek a hálózati és információs rendszerek valós biztonságát garantálják.

A NIS irányelv a kockázatokkal arányos védelem alapelve szerint rendelkezik arról, hogy a hatálya alá tartozó szereplőkre vonatkozó biztonsági követelményeknek arányosaknak kell lenniük az adott hálózati és információs rendszert érintő kockázatokkal. Ez a követelményrendszer az alapvető szolgáltatásokat nyújtó szereplőknél jelentkező kockázatoknál magasabb biztonsági igényeket rögzít, mint a digitális szolgáltatók esetében, mivel az alapvető szolgáltatók működőképességének fenntartása elengedhetetlen a kritikus társadalmi és gazdasági tevékenységek fenntartásához.

Ha az érvényesített biztonsági követelmények ellenére olyan biztonsági esemény következik be, amely ténylegesen kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára,[95] szükséges lefolytatni az adott biztonsági esemény észlelését, elemzését és elszigetelését, valamint az eseményre való reagálást biztosító és támogató eljárásokat[96] (például PreDeCo-elv).

A NIS irányelv az alapvető szolgáltatást nyújtó szereplőkre és a digitális szolgáltatókra elsődlegesen a jelentős zavart okozó biztonsági események bejelentési kötelezettségét írja elő, azzal, hogy a zavar jelentőségének meghatározásához a tagállamoknak ágazatközi és ágazatspecifikus tényezőket kell figyelembe venniük.

Ágazatközi tényezőknek minősülnek legalább az alábbiak:

- az érintett szervezet által nyújtott szolgáltatásokat igénybe vevő felhasználók száma (akár közvetlenül, akár közvetetten – például digitális szolgáltatón mint közvetítőn keresztül – veszik igénybe az adott szolgáltatást);
- az adott szolgáltatást nyújtó szereplők függelmi helyzete a jelentős zavart okozó biztonsági eseménnyel érintett szervezet által nyújtott szolgáltatásoktól;
- a biztonsági események hatása – mértéküket és időtartamukat tekintve – a gazdasági és társadalmi tevékenységekre vagy a közbiztonságra;
- a jelentős zavart okozó biztonsági eseménnyel érintett szervezet piaci részesedése;
- az adott biztonsági esemény által esetlegesen érintett terület földrajzi kiterjedése;
- a jelentős zavart okozó biztonsági eseménnyel érintett szervezet jelentősége a szolgáltatás elégséges szintjének fenntartásában, figyelembe véve az adott szolgáltatás nyújtásához rendelkezésre álló egyéb lehetőségeket is.[97]

A CSIRT-ek feladatkörébe tartozik:

- a biztonsági események nemzeti szintű monitoringja;
- a kockázatokkal és biztonsági eseményekkel kapcsolatos korai előrejelzés, riasztás, bejelentéstétel és információterjesztés a releváns érdekeltek számára;
- reagálás a biztonsági eseményekre;

[94] NIS 4. cikk, 2. pont.
[95] NIS irányelv 4. cikk, 7. pont.
[96] NIS irányelv 4. cikk, 8. pont.
[97] NIS irányelv 6. cikk, (1) bekezdés.

- kockázat- és eseményelemzés, valamint helyzetkép nyújtása;
- a CSIRT-ek hálózatában való részvétel.

Ha a CSIRT-ek a nemzeti intézményektől nem kapják meg közvetlenül a biztonsági eseményekről szóló bejelentéseket, úgy az intézményeknek hozzáférést kell biztosítani számukra az alapvető szolgáltatásokat nyújtó szereplők, illetve a digitális szolgáltatók által bejelentett biztonsági események adataihoz.

Tagállami és uniós szinten egyaránt megvalósul az együttműködés: stratégiai szinten a tagállamok, az Európai Bizottság és az ENISA képviselőiből álló együttműködési csoport[98] keretében, operatív szinten a CSIRT-ek hálózatán[99] belül (például biztonsági eseményre vonatkozó információk megosztása).

Felhasznált irodalom

03/2014 sz. vélemény személyes adatok megsértése bejelentéséről (WP213). A 29. cikk szerinti Adatvédelmi Munkacsoport kiadványa, 2014. Elérhető: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_hu.pdf (a letöltés ideje: 2017. április 7.)

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. Article 29 Data Protection Working Party, 2017. Elérhető: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 (a letöltés ideje: 2017. április 20.)

Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér. Elérhető: http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=hu (a letöltés ideje: 2017. április 20.)

Baranya Zsolt (2016): A belső adatvédelmi felelős és az elektronikus információs rendszerek biztonságáért felelős személy feladatainak összehasonlítása és a feladatok ellátásának összefüggései. *Infokommunikáció és Jog,* XIII évf. 2. sz., 66–67.

Cavoukian, Ann (2016): *Embed Privacy by Design, or Risk Losing Privacy Forever.* Berkeley Center for Law & Technology. Elérhető: www.law.berkeley.edu/wp-content/uploads/2016/03/Ann-Cavoukian.pdf (a letöltés ideje: 2017. március 20.)

Workshop on the Economic Benefits of PETs. Európai Bizottság, 2009. Elérhető: http://ec.europa.eu/justice/news/events/workshop_pets_2009/report_en.pdf (a letöltés ideje: 2017. április 17.)

Digitális Menetrend: A Bizottság akcióterve az európai jólét fellendítésére. Európai Bizottság, 2010. Elérhető: http://europa.eu/rapid/press-release_IP-10-581_hu.htm (a letöltés ideje: 2017. április 20.)

Sajtóközlemény. A Bizottság uniós adatvédelmi reformjáról született megállapodás fellendíti a digitális egységes piacot. Európai Bizottság, 2015. Elérhető: http://europa.eu/rapid/press-release_IP-15-6321_hu.htm (a letöltés ideje: 2017. április 20.)

Kiss Attila (2013): A privátszférát erősítő technológiák. *Infokommunikáció és Jog,* X. évf. 3. sz., 56.

Megjelent a hálózati és információs rendszerek biztonságáról szóló EU-s irányelv. Kormányzati Eseménykezelő Központ, 2016. Elérhető: www.cert-hungary.hu/nis_directive (a letöltés ideje: 2017. április 22.)

Muha Lajos – Krasznay Csaba (2014): *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest, Nemzeti Közszolgálati Egyetem.

Reidenberg, Joel. R. (1998): Lex Informatica: The Formulation of Information Policy Rules Through Technology. *Texas Law Review,* 1998/3.

Górniak, Sławomir – Ikonomou, Demosthenes – Tirtea, Rodica – Rockelmann, Andreas – Budd, Joshua – Vorisek, Michael (2011): *Data breach notifications in the EU.* ENISA. Elérhető: www.enisa.europa.eu/publications/dbn (a letöltés ideje: 2017. április 20.)

Szádeczky Tamás (2012): *The role of the technology. Auditing and certification in the field of data security.* In: Szőke Gergely László (ed.): *Privacy In The Workplace. Data Protection Law and Self-Regulation in Germany and Hungary.* Budapest, HVG-ORAC.

Szádeczky Tamás (2013): Az IT biztonság szabályozásának konfliktusa. *Infokommunikáció és jog,* X. évf. 56. sz., 149–153.

Székely Iván (2008): Privátszférát erősítő technológiák. *Információs Társadalom,* 8. évf. 1. sz. 20–34.

Szőke Gergely László (2017): Értesítési kötelezettség az adatvédelmi incidensek esetén – elméleti és gyakorlati kérdések. *JURA,* 23. évf. 1. sz., 140–153.

[98] NIS irányelv 11. cikk.
[99] NIS irányelv 12. cikk.

3. A NEMZETI KIBERVÉDELMI INTÉZET SZEREPE AZ ESEMÉNYKEZELÉSBEN

Marsi Tamás

3.1. A Nemzeti Kibervédelmi Intézet és szerepe az eseménykezelésben, valamint a sérülékenységvizsgálati tevékenységben

3.1.1. A kibertér és fenyegetései

A kiberfenyegetések komplexitása és jelentősége a 21. században a technika fejlődésével és elterjedésével együtt folyamatosan növekszik, a kiberbűnözésből származó károk világszinten egyre nagyobb összegre rúgnak. Ezzel párhuzamosan egyre erőteljesebb az állami szereplők fellépése, és a vélhetően államilag támogatott kiberkémkedési műveletek.

A kiberbűnözés fő célja a pénzügyi és a személyes adatok tömeges megszerzése, a pénzügyi rendszerek befolyásolása és ezzel anyagi haszon vagy üzleti előny szerzése. A személyes, pénzügyi adatok kibertámadások révén történő megszerzése nem új jelenség, de a módszerek összetétele változó trendet mutat.

Korábban a potenciális áldozatokat közvetlenül megcélozva (például megtévesztő vagy fertőzött e-mail, hamis vagy módosított weboldal) kis volumenben gyűjtöttek leginkább érzékeny adatokat, manapság azonban egyre több nagy horderejű, központi nyilvántartás elleni sikeres támadás lát napvilágot, melyekkel százezres, egyes esetekben milliós nagyságrendben jutnak személyes adatokhoz az illetéktelenek.

Az adatlopáson túl elterjedt az elektronikus szolgáltatások károkozási célú megbénítása (például elosztott szolgáltatások megtagadásával járó támadásokkal), illetve kéretlen levelek és kártékony kódok terjesztése, robothálózatok (fertőzött gépekből álló, kártékony célra felhasználható hálózatok) létrehozása és folyamatos üzemeltetése.

A kiberbűnözés mellett jelentős fenyegetésként jelent meg a *hacktivizmus,* amely jellemzően ideológiai motivációjú támadásokat takar, valamilyen eszme közvetítése vagy elérése érdekében.

Jelentős és egyre növekvő veszélyt jelentenek azok a jellemzően kiberkémkedési célú, jól szervezett, alapos és nagy szakértelemmel elrejtett támadások, melyek mögött feltételezhetően állami szereplők állnak. A fő veszélyt a rendkívül szofisztikált támadások jelentik: így hosszú időn át rejtve tudják végezni tevékenységüket, miáltal rendkívül hatásosan hajtják végre a megbízók által kijelölt célokat. Az ilyen jellegű összetett támadások célja az információszivárogtatás, a rombolás és a kémkedés.

A modern kor velejárójaként jelentkező kihívásokra válaszul jött létre a kiberbiztonság, mely a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő tevékenység, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva azt megbízható környezetté alakítják, a társadalmi és gazdasági folyamatok zavartalan működtetéséhez.[1]

[1] 2013. évi L. törvény, 1. § 26. pont.

A kibervédelem – ezt támogatandó – a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertérképességek megőrzését is.[2]

A globálisan összekapcsolt, decentralizált, dinamikusan növekvő elektronikus információs rendszerek, valamint az ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét *globális kibertérnek*[3] nevezzük.

A magyar kibertér a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak. A hazai kibertér részei továbbá a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország is érintett.[4]

3.1.2. A Nemzeti Kibervédelmi Intézet

Ezekre a kihívásokra reagálva, a kiberbiztonság növelése, az egységes és hatékony, párhuzamosságokkal kevésbé tagolt kibervédelmi struktúra megteremtése érdekében jött létre a Nemzeti Kibervédelmi Intézet (NKI).

Az NKI legfőbb feladata és célja tehát, hogy Magyarország egy összehangolt, szervezett tevékenység keretében legyen képes a modern kor egyik legnagyobb kihívásának, a kiberbiztonság megteremtésének és erősítésének az élharcosa és a kibervédelem letéteményese lenni, a globális és a hazai kibertérből érkező fenyegetéseket hatékonyan kezelni, azok megelőzésére szakszerű segítséget nyújtani.

Kiemelten fontos nemzeti érdek a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága.

Ezenkívül társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme.[5]

3.1.2.1. Történet és megalakulás

A nemzeti CERT (Computer Emergency Response Team) magyarországi kiemelt szerepét, a hálózatbiztonsági incidesek kezelését 2013-ig a Puskás Tivadar Közalapítvány keretein belül működő Nemzeti Hálózatbiztonsági Központ látta el. A feladatot az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény hatálybalépésével, 2013. július elsejével a Nemzetbiztonsági Szakszolgálat szervezetén belül létrejött Kormányzati Eseménykezelő Központ vette át, folytatva és fejlesztve a tevékenységet, megőrizve a nemzetközi vérkeringésben betöltött szerepet.

Ezzel egy időben, a Nemzeti Fejlesztési Minisztérium szakmai irányításával létrejött a Nemzeti Elektronikus Információbiztonság Hatóság (NEIH), amely hatósági jogkör birtokában végezte az informatikai rendszerek megfelelőségének vizsgálatát és az egyéb szakmai feladatokat. A szakhatósági, tehát a biztonsági tesztelési, sérülékenységvizsgálati feladatokat a Közigazgatási és Igazságügyi Minisztérium irányításával működő Nemzeti Biztonsági Felügyelet szervezetén belül elhelyezkedő Elektronikus Biztonsági Intelligencia Központ (CDMA) végezte. Ez a három különálló szervezet, a GovCERT, a NEIH és az NBF-CDMA jelenítette meg a struktúra operatív elemét.

---

[2] 2013. évi L. törvény, 1. § 27. pont.
[3] 2013. évi L. törvény, 1. § 22. pont.
[4] 2013. évi L. törvény, 1. § 35. pont.
[5] 2013. évi L. törvény preambuluma.

A szervezetrendszer stratégiai szintű elemei: a Nemzeti Kiberkoordinációs Tanács mint a kormány javaslattevő, véleményező szerve, az annak keretében működő munkacsoportok, valamint a Kiberbiztonsági Fórum ebben az időben a Miniszterelnökség szakmai felügyelete alatt álltak.

2015 szeptemberében a NEIH szervezete és feladatai – a sérülékenységvizsgálati feladatokkal együtt – a Nemzetbiztonsági Szakszolgálathoz kerültek. Ekkorra már a Nemzeti Kiberkoordinációs Tanács is a Belügyminisztériumhoz tartozott, és ezzel kezdetét vette a korábbi széttagolt intézményi struktúra megszűnése.

Mivel a hatósági, a szakhatósági és az eseménykezelési tevékenység is egy szervezeten belül kapott helyet, ezen feladatok egységes megjelenése és a párhuzamosságok megszűntetése érdekében 2015. október 1-jén ernyőszervezetként megalakult a Nemzeti Kibervédelmi Intézet.

A struktúra átalakulása paradigmaváltással is együtt járt, ennek keretében az állami intézmények védelme egy meghatározott életciklus mentén valósítható meg. Az NKI létrehozásában rejlő szinergiákat kiaknázva, a rendeltetéséből fakadó egyes funkciókat rendszerbe szervezve egy komplex biztonsági szolgáltatásportfólió jött létre, amelynek eredményeként az NKI hatékonyan képes detektálni a sérülékeny pontokat az egyes intézmények működésében.

3.1.2.2. Az intézet felépítése, jogszabályi háttere

Az intézet a hatékony működés érdekében három szervezeti egységből és öt szakterületből áll. Az incidenskezelési és kapcsolódó feladatokat a Kormányzati Eseménykezelő Központ, míg a hatósági feladatokat a Nemzeti Elektronikus Információbiztonság Hatóság látja el. Ezenkívül létrejött egy harmadik, technikai támogató szervezeti egység, mely a sérülékenységvizsgálatok elvégzésével, valamint az EMIR, a FAIR és az IMIR 2014–2020 rendszerek biztonságirányításával foglalkozik. Az ötödik szakterület egyéb támogató, nemzetközi és hazai koordinációs, szolgáltató és ügyviteli tevékenységet végez. Az intézet vezetését a Nemzeti Kibervédelmi Intézet igazgatója látja el.

Az NKI működésének jogi alapját a Magyarország Biztonsági Stratégiáját, a Magyarország Nemzeti Kiberbiztonsági Stratégiáját, valamint az ez utóbbit is megalapozó, az Európai Unió kiberbiztonsági stratégiáját is alapul véve megalkotott, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.), valamint három kormányrendelet teremti meg.

A 185/2015. számú kormányrendelet a GovCERT, a 186/2015. számú kormányrendelet a NEIH, míg a 60/2014. számú kormányrendelet a biztonságirányítási szakterület jogi alapját teremti meg. A rendeletek a különböző feladatokat a Nemzetbiztonsági Szakszolgálathoz címzik, amelynek szervezetén belül kapott helyet az intézet. Ezenkívül a különböző tevékenységekhez számos más jogszabály is kapcsolódik.

3.1.3. A Kormányzati Eseménykezelő Központ

3.1.3.1. A GovCERT feladat- és hatásköre

A Kormányzati Eseménykezelő Központ legfőbb feladatait és hatáskörét az Ibtv. határozza meg. A 185/2015. kormányrendelet a Kormányzati Eseménykezelő Központ feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól rendelkezik, mely a törvény végrehajtási rendelete. Ezenkívül is számos jogszabály kapcsolódik a központ tevékenységéhez, és segíti munkáját adatkérési, valamint egyéb jogosultságok biztosítása révén.

A számítógépes eseménykezelő központ a törvény szerint az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely tagsággal és akkreditációval rendelkezik a nemzetközi hálózatbiztonsági, valamint

kritikus információs infrastruktúrák védelmére szakosodott szervezetekben. Európai használatban a CSIRT (Computer Security Incident Response Team), amerikai használatban a CERT (Computer Emergency Response Team) mozaikszó használata terjedt el.[6]

A jogszabályok alapján a GovCERT-nek több, egymástól jól elhatárolható folyamata azonosítható:

- A fenyegetettség menedzsmentfeladaton belül adatgyűjtés, adatelemzés, offline monitorozás, valamint adatmegosztás történik. Ebben a folyamatban keletkeznek a publikációk és az egyéb termékek, mint a riasztások, tájékoztató hírlevelek, rendszeres sérülékenységi tájékoztatók és a negyedéves jelentés.
- A biztonsági események kezelése, más megfogalmazásban incidenskezelés a különböző eseményeknek a keletkezést követő feldolgozása, koordinációja, technikai kivizsgálása, kapcsolattartás az ügyfelekkel, valamint a munkát megkönnyítő nyilvántartások vezetése.
- A Kormányzati Eseménykezelő Központ végzi a hatáskörébe tartozó rendszerek sérülékenységvizsgálatát, melynek célja a rendszerek gyenge pontjainak azonosítása, valamint javaslatok tétele a biztonság növelése céljából.
- A megelőző és támogató tevékenység részeként a GovCERT információbiztonsági tudatosító és tanácsadó tevékenységet végez, részt vesz Magyarország kiberkoordinációjában, valamint kibervédelmi gyakorlatokat szervez, azokban részt vesz.
- Ezeken kívül a Kormányzati Eseménykezelő Központ ellátja a nemzeti CERT feladatát is, melynek keretében nemzetközi szinten képviseli hazánkat a kibervédelemre szakosodott szervezetekben, fogadja, feldolgozza és továbbítja a belföldi és nemzetközi szintről érkező riasztásokat, és központi szerepet tölt be a veszélyek elhárításának koordinálásában.

3.1.3.2. A GovCERT ügyfelei és partnerei

A GovCERT számos intézménnyel és szervezettel tart kapcsolatot. Ezen belül megkülönböztet ügyfeleket, ágazati eseménykezelőket, kvázi ágazati eseménykezelőket, valamint hazai és nemzetközi partnereket.

A központ ügyfélköre igen nagyszámú, közel 4000 intézményből áll, a törvény rendelkezéseit ezen intézmények esetén kötelező alkalmazni.[7]

A Köztársasági Elnöki Hivatalt, az Országgyűlés Hivatalát, az Alkotmánybíróság Hivatalát, az Országos Bírósági Hivatalt, a bíróságokat, az ügyészségeket, az Alapvető Jogok Biztosának Hivatalát, az Állami Számvevőszéket, a Magyar Honvédséget, valamint a Magyar Nemzeti Bankot a törvény taxatíve felsorolja: ezeket nevezzük *törvény szerinti kiemelt ügyfeleknek.*

Ezenkívül ügyfélként szerepelnek még a minisztériumok, az önálló szabályozó szervek, a rendvédelmi szervek (a rendőrség, a büntetés-végrehajtási szervezet, a hivatásos katasztrófavédelmi szerv, a polgári nemzetbiztonsági szolgálatok), az államigazgatási szervek (az autonóm államigazgatási szervek, a kormányhivatalok és a központi hivatalok), továbbá a fővárosi és a megyei kormányhivatalok.

A központ legnagyobb ügyfélcsoportja a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatalai, valamint a hatósági igazgatási társulások.

A törvény hatálya, így a GovCERT feladat- és hatásköre a fent említett szervek számára adatkezelést végzőkre, továbbá a jogszabályban meghatározott, a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozóira is kiterjed.[8]

A GovCERT az ügyfelei esetén mind az incidenskezelés, mind az egyéb tevékenységek végzése során elsősorban a biztonságiesemény-kezelési megbízottal tartja a kapcsolatot, aki az érintett szervezet vezetője által a biztonsági események kivizsgálására hivatalosan megbízott személy.[9]

---

[6] 2013. évi L. törvény, 1. § 42. pont.
[7] 2013. évi L. törvény, 2. §.
[8] 2013. évi L. törvény, 2. § (2) bekezdés.
[9] 185/2015. (VII. 13.) kormányrendelet, 1. § 4. pont.

Magyarországon működnek úgynevezett ágazati eseménykezelő központok, melyek a jogszabályokban előírt rendszerek esetén végzik az eseménykezelést. Ezekkel a GovCERT aktív kapcsolatot tart és folyamatos együttműködést folytat.

A honvédelmi célú elektronikus információs rendszereket érintő biztonsági események és fenyegetések kezelését a MilCERT, a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereit érintő biztonsági események és fenyegetések kezelését az IntCERT végzi.[10]

A törvényben meghatározott, kijelölt létfontosságú létesítmények, rendszerek elektronikus információs rendszereit érintő biztonsági események és fenyegetések kezelését az állami és önkormányzati szervek kivételével az Országos Katasztrófavédelmi Főigazgatóságánál működő Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ (LRLIBEK) látja el.[11]

A feladatok ellátása érdekében a központ széles hazai és nemzetközi partneri hálózatot épített ki. Ezekkel a szervezetekkel és társaságokkal az együttműködést nem az Ibtv., hanem egyéb jogszabályok, illetve megállapodások teszik lehetővé.

A hazai partnerek közül kiemelendőek az úgynevezett *kvázi ágazati CERT-ek.* Több minisztérium is létrehozott olyan eseménykezelőt, ami az adott ágazat állami szereplőit igyekszik koordinálni incidenskezelési szempontból. Az ilyen központokhoz tartozó intézményekkel a kommunikáció történhet közvetlenül vagy az eseménykezelő központon keresztül is. Kvázi ágazati CERT-nek tekinthető többek között a Kormányzati Informatikai Fejlesztési Ügynökség Nemzeti Információs Infrastruktúra Fejlesztési Program (KIFÜ-NIIF) által működtetett eseménykezelő központ.

Aktív és segítő együttműködés alakult ki a fentieken túl az internetszolgáltatók, a központosított szolgáltató szerepét ellátó Nemzeti Infokommunikációs Szolgáltató Zrt., a különböző érdekvédelmi szervezetek, állami társaságok és egyéb iparági szereplők és a GovCERT között.

A hatékony nemzetközi kapcsolattartás érdekében a központ együttműködik az ENISA-val, egyéb, a külföldi eseménykezelőket tömörítő szervezetekkel (FIRST, TI, IWWN, CECSP), külföldi CERT-ekkel és CSIRT-ekkel, valamint nemzetközi iparági szereplőkkel és egyéb biztonsági szervezetekkel.

3.1.4. A fenyegetettségmenedzsment

3.1.4.1. A fenyegetésekről általában

A fenyegetettségmenedzsment célja a rendszerekben potenciálisan előforduló sérülékenységek azonosítása. A sérülékenység az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat.[12]

A fenyegetés olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemeinek védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát.[13]

A fenyegetettség az a lehetséges veszély, amely valamilyen sérülékenység kihasználásával sérti a kitűzött biztonsági célokat (bizalmasság, sértetlenség, rendelkezésre állás), és ezáltal kárt okozhat az információ tulajdonosának. A fenyegetettségmenedzsment e lehetséges veszélyek kezelése, amely *kármegelőzéssel és kárcsökkentéssel* érhető el.

Kármegelőzésről akkor beszélünk, ha a tevékenység célja a várható negatív esemény bekövetkezési valószínűségének csökkentése, annak elkerülése tehát a prevenció. Kárcsökkentés a kárhatás horderejének ellensúlyozása, tehát a korrekció. A fenyegetettségmenedzsment során az első lehetőségre helyeződik a hangsúly.

[10] 185/2015. (VII. 13.) kormányrendelet, 6. § (1)–(2) bekezdés.
[11] 185/2015. (VII. 13.) kormányrendelet, 6. § (3) bekezdés.
[12] 2013. évi L. törvény, 1. § 40. pont,
[13] 2013. évi L. törvény, 1. § 19. pont,

A folyamat célja a kármegelőzésen és a kárcsökkentésen kívül a biztonsági események kezeléséhez szükséges információk begyűjtése, feldolgozása és megosztása.

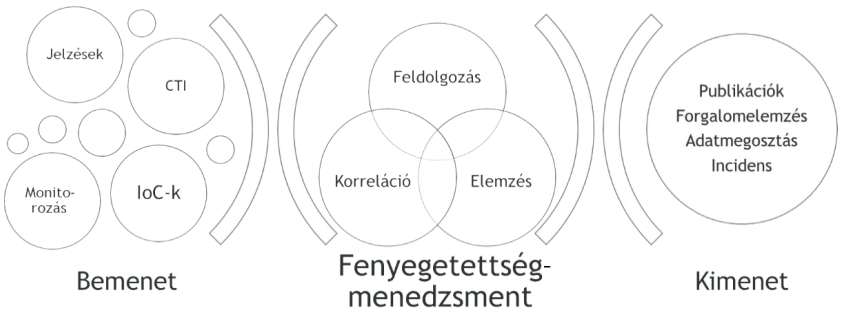
A központ a biztonsági események megelőzése céljából az állami és önkormányzati szervek elektronikus információs rendszereit érintő fenyegetésekkel összefüggő tájékoztatási és tudatosítási feladatokat lát el.[14]

Ennek szellemében a GovCERT az elektronikus információs rendszereket veszélyeztető sérülékenységekkel és fenyegető kockázatokkal összefüggésben ellátja az elektronikus információs rendszerek biztonságáért felelős személyek tájékoztatását, a hatóságok és az eseménykezelő központok tájékoztatását, továbbá rendszeres tájékoztatást nyújt a honlapján a sérülékenységekről és fenyegetésekről, valamint a javasolt biztonsági intézkedésekről.

A Kormányzati Eseménykezelő Központ elemzéseket, jelentéseket készít a magyar és nemzetközi információbiztonsági irányokról, negyedévente jelentést tesz a hatáskörébe tartozó biztonsági eseményekről a Nemzeti Kiberbiztonsági Koordinációs Tanácsnak, valamint évente jelentést készít tevékenységéről a központot irányító miniszter számára.

3.1.4.2. A fenyegetettségmenedzsment folyamata

A folyamaton belül meg kell valósítani az adatok feldolgozását, korrelációját és elemzését, valamint az információk megosztását. A tevékenység keretében a begyűjtött adatok körét folyamatosan karban tartani és bővíteni szükséges, a keletkezett termékeket az előállításon túl a trendeknek valamint az ügyfelek igényeinek megfelelően fejleszteni szükséges.



1. ábra

A fenyegetettségmenedzsment folyamata a Kormányzati Eseménykezelő Központnál

*Forrás:*A szerző saját szerkesztése

A feldolgozás egy folyamatos, 24 órás feladatvégzés, melyet elsősorban a GovCERT információbiztonsági ügyelete, valamint egyéb szakemberek végeznek. A feldolgozás lehetőség szerint automatikusan, ütemezetten, kifejezetten az adott tevékenység támogatására készült szakrendszerek használatával történik. Előnyben részesülnek a nyílt forráskódú (open source) eszközök, de egyes feladatok elvégzéséhez egyedi megoldások alkalmazása szükséges.

A korreláció az érintteti kör azonosítása, az események intézményhez, szolgáltatóhoz rendelése, melynek elsődleges adata az IP-cím.

Az adatok elemzésére szükség szerint kerül sor, számos adat elemzés nélkül is felhasználható. Mivel az adatok egyes esetekben nagy tömegben, strukturáltan állnak rendelkezésre, lehetőség van szignifikancia- és relevanciavizsgálatok, összehasonlító elemzések és trendelemzések készítésére. Ezek alapján további adatbegyűjtésre is sor kerülhet. A tények és a következtetések megállapításán túl az elemzés célja a falspozitívok és a falsnegatívok kiszűrése is.

[14] 185/2015. (VII. 13.) kormányrendelet, 5. § (1)–(3) bekezdés.

3.1.4.3. A fenyegetettségmenedzsment bemenete

A fenyegetettségmenedzsment folyamatának bemenetei olyan releváns információk, melyek a központ számára nyers, valamilyen jellegű további feldolgozást igénylő formában állnak rendelkezésre, és ezen tevékenységet követően hasznosíthatóak a központ, az ügyfelei és a partnerei részére.

A *jelzések* a GovCERT, valamint az állami és önkormányzati partnerei számára releváns szoftversérülékenységek, a káros kódok leírásai, valamint egyéb információk, például újszerű támadástípusok.

Az információk főszabályként nyílt hozzáférésűek, szoftver- és hardvergyártók leírásai, antivíruscégek publikációi, sérülékenységet gyűjtő portálok aggregát információi, informatikai szakportálok releváns cikkei. A jelzésekkel kapcsolatos legfőbb feladat az adatok gyűjtése, becsatornázása, strukturálása, feldolgozása és hasznosítása.

A központ a jelzések hatékony feldolgozásához a holland CERT TARANIS nevű alkalmazást használja, mely alkalmas a jelzések gyors, automatizált és ütemezett begyűjtésére, feldolgozása. A rendszer alkalmas továbbá a jelzések folyamatalapú kezelésére és egy meghatározott sémához történő illesztésére.

Lehetőség van úgynevezett *inventory,* tehát szoftverleltár felvitelére is, mely megkönnyíti a releváns tartalmak kiválasztását. A rendszer több mint 300 adatforrással, több mint ezer jelzéssel dolgozik.

A jelzések feldolgozásának folyamata az automatizált begyűjtéssel kezdődik, amire több protokoll, adatstruktúra is használható (például Html, Xml, Pop3, Imap). Ezt követően kerül sor a kiválasztásra, melyhez indexelt kereső áll rendelkezésre.

A publikálásra kiválasztott jelzés elemzésének része a további információk begyűjtése, a jelzések összekapcsolása és az információk összegzése. A munkafolyamatban lehetőség van a feladatok megosztására is.

A publikáció elkészítése, megírása az információk strukturálásával kezdődik. Az elemzés során begyűjtött információkat egy meghatározott sémához kell illeszteni, melyben a publikációhoz metaadatokat kell hozzárendelni egy előre meghatározott listából. Olyan adatok megadása szükséges, mint érintett rendszerek, érintett verziók, hatás, kockázati besorolás, a kihasználáshoz szükséges hozzáférés, illetve a támadás típusa. A kockázati besorolás elvégzése a CVSS (Common Vulnerability Scoring System) szabályai szerint történik.

Ebben a munkafolyamatban történik a publikáció véglegesítése és ellenőrzése is. Az elkészült munka ellenőrzése szakmai és stilisztikai szempontok alapján történik.

A publikálás, vagyis a weboldalra helyezés és az érintettekhez juttatás a fenyegetettségmenedzsment folyamatának egyik kimenete.

A *CTI, vagyis Cyber Threat Intelligence* rendszerezett, elemzett és finomított adatok, a rendszerek biztonsága szempontjából releváns információk összessége. Olyan adatok, melyekkel biztonsági események, azok potenciális veszélye tárható fel. Segít megérteni és kezelni a különböző kockázatokat, mint a célzott támadás (APT) vagy a fel nem fedezett sérülékenységek (0-day).

A CTI-adatok általában adatgyűjtő eszközökből, csapdarendszerekből (honeypot), rendszerek és védelmi eszközök (IPS/IDS) naplóállományaiból, netflow és nyers hálózati forgalmi adatokból, valamint hálózati felderítő tevékenységből származnak.

Sok szervezet az ilyen eszközökből szerzett információt elérhetővé teszi egy-egy közösségen belül. Külső szereplők is szolgáltatnak ilyen jellegű adatokat, akár szolgáltatásként, akár nonprofit tevékenységként.

A nyers logadatok begyűjtésére, feldolgozására, tárolására és elemzésére a GovCERT egy Hadoop rendszerű Big Data-rendszert használ, mely elosztott számítási és tárolási kapacitást és magas rendelkezésre állást biztosít, az adatbázisban sztenderd SQL-lekérdezések futtathatóak, a komponensek többsége nyílt forráskódú.

A Shadowserver egy nemzetközi nonprofit szervezet, különböző, változatos adatgyűjtési technológiákkal, amely több mint harminc típusú adatsort oszt meg a GovCERT-tel a teljes hazai

IP-címtartományról.[15] A legjobban hasznosítható adatok a botnet vezérlőszerveri információk, a sérülékeny nyitott hálózati portok, valamint egyéb sérülékenységi információk.

A CERT-EU, az európai CERT szerepét betöltő szervezet is végez adatgyűjtést és adatmegosztást. A leggyakrabban megosztott információk közé tartoznak a robothálózati vagy zombihálózati (botnet) információk, az adathalász oldalak és a Tor kijárati pontok (exit node) listája.

A SPAMHAUS egy nemzetközi monitorozó szervezet, mely robothálózatok jelenlétének nyomait kutatja a kibertérben. A BLOCKLIST egy olyan nemzetközi önkéntes adatgyűjtő szervezet, ami támadó IP-címek gyűjtésére specializálódott.

Az *IoC (indicator of compromise) vagy támadási vektor* a CTI-hoz közeli, azon belül található fogalom. Az IoC a hoston vagy a hálózatban olyan konkrét behatolásra utaló jel, amely nagy valószínűséggel jelzi a sikeres támadást. Az adatok megkönnyítik a különböző kártevők, sérülékenység-kihasználások detektálását a rendszerben.

Az ilyen adatok mindig mély szakmai vizsgálat, incidenskezelési tevékenység, kártevő elemzés eredményeként állnak elő. A legtipikusabb IoC-k az IP, a domain, a fájllenyomat (hash). Nagyon hasznos, ha a domain helyett URL-t, a manapság még mindig használt, de nem biztonságos MD5 hash helyett két különböző típusú lenyomatot rögzítenek. Ezenkívül a támadás azonosításához hasznosak lehetnek az esemény során keletkezett registry értékek, a fájlrendszer-változások és a támadó által használt e-mail-cím is.

A megszerzett információkat a különböző szervezetek elsősorban bizalmi alapon osztják meg egymással. A Malware Information Sharing Platform (MISP) egy olyan nyílt forráskódú, webes alapú rendszer, amely ehhez biztosít felületet. Lehetőség van közösség létrehozására, meglévő közösségekhez való csatlakozásra. A rendszer támogatja az adatok gyors, hatékony feldolgozását és megosztását, strukturált tárolását, a titkosítások használatát, valamint segítségével több ismert formátumban lehetséges az adatok exportja is.

A Kormányzati Eseménykezelő Központ a napi munkája során rendszeresen és konkrét eseményhez kötődően is végez *monitorozási tevékenységet.* Mivel a GovCERT aktív eszközöket (például portscan) nem használhat, ezért a kutatás speciális eszközök és adatbázisok segítségével történik.

Folyamatos tevékenység a weboldalrongálás (deface) aktív keresése a kibertérben, ezzel párhuzamosan különböző offline eszközök segítségével elavult, sérülékeny tartalomkezelők keresése is. Ezenkívül eseti jelleggel a sérülékenységek kihasználhatóságának kutatása is zajlik, úgynevezett offline monitorozó eszközök segítségével, melynek keretében az érintett eszközök, az aktív szolgáltatások keresése zajlik.

3.1.4.4. A fenyegetettségmenedzsment kimenete, termékei

A folyamat eredményeként előállnak különböző termékek és egyéb intézkedési lehetőségek keletkeznek. Ezek a publikálás, a hálózati forgalomelemzés kezdeményezése, az adatmegosztás ügyfelekkel és partnerekkel, valamint a biztonsági incidens keletkezése.

A *publikálás* egy olyan munkafolyamat, amelyben az adatok aggregálását és elemzését követően egy új, önálló termék keletkezik, melynek célja az ügyfelek és a partnerek tájékoztatása. A publikálás az esetek döntő többségében a jelzésgyűjtési folyamat végterméke.

A központ által karbantartott, technikai témákkal foglalkozó weboldalon, a tech.cert-hungary.hu-n napi rendszerséggel jelennek meg sérülékenységi publikációk, káros kódok leírásai, egyéb biztonsági események összefoglalása, javaslatok, valamint különböző fenyegetések leírása.

A tájékoztatók előre meghatározott rendszeres időközönként, különböző gyakorisággal (például naponta, hetente) és más-más részletességi szinttel készülnek az ügyfelek és a partnerek számára.

[15] www.shadowserver.org/wiki/pmwiki.php/Shadowserver/Mission (a letöltés ideje: 2017. április 20.)

Az anyagok a sérülékenységi információk összefoglalását, egyéb incidensinformációkat és statisztikákat tartalmaznak.

A riasztás és a tájékoztató hírlevél célja a figyelem felhívása egy konkrét problémára. Ezeket a termékeket az úgynevezett riasztási címlistán szereplő ügyfelek és partnerek közvetlenül, e-mailben kapják meg.

A riasztás olyan esetekben készül, ha a GovCERT egy releváns, az államigazgatásban elterjedt szoftvert, hardvert érintő magas vagy kritikus sérülékenységről szerez tudomást, amely távolról, autentikáció nélkül és/vagy könnyen kihasználható, és aktívan ki is használják. A riasztás röviden és tömören írja le a problémát, általában megoldási javaslatot is kidolgoznak, a cél a figyelemfelhívás, a megoldás elősegítése.

A tájékoztató hírlevél hasonló értesítési körnek szánt termék, melyben leginkább nem konkrét sérülékenységek, hanem trendek, fenyegetések és potenciális veszélyek leírása történik.

A Kormányzati Eseménykezelő Központ a Nemzeti Távközlési Gerinchálózatban (NTG) a Nemzeti Infokommunikációs Szolgáltató Zrt. (NISZ) közreműködésével hálózati forgalomelemzéseket és tiltásokat kezdeményez.

A fenyegetettségmenedzsment keretében feldolgozott és elemzett CTI-információk és IoC-adatok alapján a NISZ határvédelmi rendszerén történnek a keresések, melyek eredményeként az egy-egy káros tevékenységhez köthető intézmények is feltárásra kerülhetnek.

Indokolt esetben a potenciálisan káros IP-címek és domainnevek NTG-ből történő kitiltására is sor kerülhet, melynek segítségével a káros tevékenység megelőzhető, az okozott kár csökkenthető.

A folyamatban előálló adatokat és információkat napi és heti rendszerességgel ütemezetten, lehetőség szerint automatizáltan, hatáskör és illetékesség alapján, állami és nem állami partnerek részére is megosztják.

Az esetek többségében a különböző típusú CTI-adatokat küldik meg a Nemzeti Média- és Hírközlési Hatóságnak, az Internet Szolgáltatók Tanácsának támogatásával működő Hun-CERT-nek, valamint együttműködési megállapodás alapján két internetszolgáltatónak.

A folyamat egyik igen gyakori kimenete a *biztonsági esemény,* mely speciális szempontok szerint jön létre, és amelyet részletesen elemzünk majd a biztonsági eseményeket taglaló részben.

3.1.5. A biztonsági események kezelése

3.1.5.1. A biztonsági eseménnyel kapcsolatos alapfogalmak

A biztonsági események kezelésének megértéséhez szükséges tisztázni az ezzel kapcsolatos alapfogalmakat, melyek segítenek eligazodni a folyamatok és az abban használt kifejezések között.

A biztonsági esemény a törvény szerint egy olyan nem kívánt vagy nem várt esemény, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.[16] A Kormányzati Eseménykezelő Központ a belső szabályozásában is ennek megfelelően definiálja a biztonsági esemény, más néven az *incidens* fogalmát. Tehát a fenyegetettség egy lehetséges, az incidens pedig egy bekövetkezett esemény.

A biztonsági esemény kezelése az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység.[17]

[16] 2013. évi L. törvény, 1. § 9. pont.
[17] 2013. évi L. törvény, 1. § 10. pont.

A GovCERT az átlagostól eltérő, speciális incidenskezelő tevékenységet végez. A szervezetek általában a saját biztonsági incidenseiket kezelik, azonban a központ más szervezetek, egy dedikált ügyfélkör eseményeit koordinálja, elemzi és ad tanácsot azok kezelésére, elhárítására és megelőzésére.

A GovCERT gyakorlatában egy biztonsági incidens egy intézménnyel kapcsolatos esemény (bejelentés, észlelés vagy jelzés), melynek legfőbb tulajdonságai (metaadatai) *a típus, a kockázati besorolás és a kampányhoz kötöttség.* Szintén fontos adatok *az indikátorok* (például IP, domain) és *a kapcsolattartó személyek*. Az eseménykezelést intézményenként elkülönült kommunikáció, önálló kockázati besorolás, a többi eseménytől elszeparált vizsgálat és egyedi javaslatok jellemzik.

Az incidenskezelés három különböző szintre tagolódik, melyeket a későbbiekben részletesen ismertetünk:

1. első lépésben a rögzítés és az első műveletek, vizsgálatok történnek meg,
2. második lépésben koordináció, kapcsolattartás és adatelemzés történik,
3. a harmadik lépés nagy mennyiségű adat és információ mély technikai kivizsgálását foglalja magában.

Az incidenskezelés megkönnyítése és áttekinthetősége érdekében a Kormányzati Eseménykezelő Központ egy erre a célra rendszeresített, kifejezetten incidenskezelés támogatására készült hibajegykezelő (ticketing) rendszert használ, az RTIR-t. Az alkalmazás segítséget nyújt az incidensek teljes életciklusának nyomon követésére, az NKI által használt életciklus menedzselésére. Az intézményekkel folytatott írásbeli kommunikáció minden esetben itt történik: külön hibajegy (ticket) típusban a bejelentőkkel és egyéb információforrásokkal (Incident Report), valamint külön típusban az intézménnyel és egyéb érintettel, például szolgáltatókkal (Investigation). A kommunikációs jegyeket minden esetben egy harmadik típusú jegy (Incident) fogja össze, melyben az incidens metaadatait is tárolják. Az Incident Report és az Investigation ennek a „gyerekeként" (children) fogható fel. Az egyéb kommunikációk, intézkedések, megállapítások rögzítése szintén az Incidentben történik.

Az incidensek típusának meghatározására a Kormányzati Eseménykezelő Központ az ENISA (Az Európai Unió Hálózat- és Információbiztonsági Ügynöksége) által kidolgozott rendszer egy módosított változatát használja.[18] A módosítás oka, hogy ebben a kétszintű kategóriarendszerben a magyar gyakorlat szerint nem minden esemény minősül biztonsági incidensnek (ilyen például a kéretlen levél), így ezek a kategóriák nincsenek használatban.

A taxonómiarendszer nyolc fő- és 25 alkategóriát tartalmaz:

1. Káros kód (például vírus, féreg, trójai).
2. Információgyűjtés (például portscan, social engineering).
3. Behatolási kísérlet (például sérülékenység kihasználása, bejelentkezési kísérlet).
4. Behatolás (például fiók kompromittálódása, alkalmazás kompromittálódása, bot).
5. Elérhetőség (például DoS, DDoS).
6. Csalás (például phishing).
7. Sérülékenység (például open resolver).
8. Egyéb.

Az incidensek kockázati besorolására egy ötfokozatú skálát vezettek be. A kockázati besorolás legfontosabb következménye *az incidensre adott érdemi reakció ideje.* Minél magasabb egy incidens besorolási szintje, annál gyorsabban szükséges arra reagálni. A kockázati besorolás több körülménytől is függ, melyet egy mátrix tartalmaz. Ennek a legfontosabb eleme a biztonsági esemény szervezetre gyakorolt hatása, amely lehet minimális, alacsony, közepes, magas és kritikus.

A Kormányzati Eseménykezelő Központ csak a korábban részletesen ismertetett, törvényben meghatározott ügyfelek esetén végezhet incidenskezelési tevékenységet, erre terjed ki a hatásköre; ezeket

[18] www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies (a letöltés ideje: 2017. április 20.)

„állami és önkormányzati" szerveknek nevezzük, minden más szereplő az úgynevezett „nem állami" kategóriába tartozik.

A *kampány* egy speciális incidenskezelési fogalom. Adott esetben több biztonsági esemény keletkezik, mely egy kiváltó okhoz (vagy azok szoros összefüggéséhez) vezethető vissza, ugyanaz vagy hasonló indikátorok (IoC) jellemzik. Ebben az esetben az incidensek típusa nagy valószínűséggel ugyanaz lesz, azonban a kockázati besorolás az incidens szervezetre gyakorolt hatásától és egyéb körülményektől függően eltérő lehet. Ezeket az eseményeket együttesen, egymással párhuzamosan kell kezelni. Egy kampány-összefoglaló nyilvántartás vezetése is elvárás, azonban a kommunikáció intézményenként elkülönülten zajlik. A tudomásra jutást követően általában riasztást vagy tájékoztatást adnak ki, az események lezárását követően pedig összefoglaló jelentés is készülhet.

Az ügyfelekkel való folyamatos kapcsolattartás egy formalizált tevékenység, mely többek között egy kapcsolattartói adatbázis folyamatos frissítését és karbantartását foglalja magában. Az adatbázis tartalmazza az intézmény adatait, elöd- és utódszervezeteit, az incidenskezelési megbízott adatait, nevét, telefonszámát, elektronikus elérhetőségét, az ágazati eseménykezelőhöz tartozást, az IP-címeinek és domainneveinek listáját, valamint a termékre feliratkozásait, ezenkívül egyéb adatok felvitelére is lehetőség van.

3.1.5.2. A biztonsági események kezelésének alapszabályai

Az incidensek kezelésének alapszabályait a 2013. évi L. törvényben adott felhatalmazás alapján a 185/2015. számú kormányrendelet fekteti le, mely rendelkezik az intézmények és a központ jogairól és kötelességeiről, valamint egyéb lehetőségekről is.

A biztonsági esemény kivizsgálásában elsősorban az elektronikus információs rendszer biztonságáért felelős személy, a biztonságiesemény-kezelési megbízott és a hatáskörrel rendelkező eseménykezelő központ vehet részt.[19]

Az eseménykezelési tevékenység öt egymástól jól elhatároltató cél miatt fontos. A bekövetkezés okainak feltárása a legfontosabb, azonban az érintett rendszerek behatárolásának is nagy jelentősége van. Ezt követően kerül sor az elhárítási javaslat kidolgozására, a tapasztalatok megosztására és a megelőzési tevékenységre.[20]

A nemzetbiztonsági védelem alá eső intézmények esetén az elektronikus információs rendszer biztonságáért felelős személy, valamint a biztonságiesemény-kezelési megbízott kinevezésének, illetve megbízásának hatálybalépését 30 nappal megelőzően a Kormányzati Eseménykezelő Központot véleményezési jog illeti meg.[21]

A GovCERT ügyfelei kötelesek a központ részére az elektronikus információs rendszereiken bekövetkezett biztonsági eseményeket haladéktalanul bejelenteni. Ezenkívül a szervezetek kötelesek a biztonsági események kezeléséhez szükséges műszaki, technikai adatokat, információkat összegyűjteni és elektronikus formában átadni vagy azokat egyéb módon hozzáférhetővé tenni.[22]

Ha a biztonsági eseménnyel érintett szervezet bármely okból nem képes az adatok összegyűjtésére, a központ begyűjtheti azokat. A biztonsági eseménnyel érintett szervezet gondoskodik arról, hogy a központ az adatokhoz hozzáférjen.[23]

A GovCERT a biztonsági eseményben érintett szervezettel szorosan együttműködve dolgozza ki a biztonsági esemény felszámolásához szükséges intézkedéseket, amelyeket a biztonsági eseménnyel érintett szervezet köteles végrehajtani.[24]

[19] 185/2015. (VII. 13.) kormányrendelet, 8. §.
[20] 185/2015. (VII. 13.) kormányrendelet, 12. §.
[21] 185/2015. (VII. 13.) kormányrendelet, 9. §.
[22] 185/2015. (VII. 13.) kormányrendelet, 10. § (1)–(2).
[23] 185/2015. (VII. 13.) kormányrendelet, 10. § (3).
[24] 185/2015. (VII. 13.) kormányrendelet, 10. § (4).

A központ a biztonsági eseményről szigorúan zárt kezelésű technológiai naplót vezet, amely egyéb statisztikai adatokon kívül tartalmazza a biztonsági esemény kivizsgálásának támogatása során tett intézkedéseket és azok eredményét is.[25]

Az összegyűjtött és átadott információk alapján a GovCERT a biztonsági eseményekre utaló jeleket folyamatosan elemezi, értékeli, és folyamatos (7/24) ügyeleti rendszerén keresztül értesíti az elektronikus információs rendszer üzemeltetőjét a biztonsági esemény bekövetkeztének veszélyéről vagy fennállásáról, valamint a javasolt intézkedésekről.[26]

Az incidenskezelés kapcsán a központ és a központosított informatikai és elektronikus hírközlési szolgáltató – mely feladatra a Nemzeti Infokommunikációs Szolgáltató Zrt.-t (NISZ) jelölték ki – szoros kapcsolatban áll egymással.

Ebből is adódóan a NISZ a központ által vezényelt biztonságiesemény-kezelés során köteles a biztonsági eseményben érintettek (támadó/támadott) azonosításához szükséges műszaki, technikai adatok átadására a központnak, az ismert fenyegetések elleni védelmi intézkedések, műszaki, technikai megoldások alkalmazására, a központ kérésére adatok szolgáltatására a hálózati forgalomba való beavatkozásra utaló jelek elemzése, értékelése céljából, valamint a központ által meghatározott, biztonsági eseményekkel kapcsolatos feladatokban együttműködni.[27]

A GovCERT előtt álló lehetőség a biztonsági események kivizsgálása nem állami szereplők bevonásával. Az elektronikus hírközlési szolgáltató konkrét incidens kivizsgálásakor együttműködik a központtal az Ibtv.-ben foglalt feladatainak ellátása érdekében. Ennek keretében a szolgáltató értesíti a GovCERT-et, ha biztonsági eseményt vagy fenyegetettséget észlel, valamint értesíti az ügyfelét, ha rendszere biztonsági eseményhez köthető, azt okozza vagy fenyegeti.[28]

3.1.5.3. Biztonsági események keletkezése

A biztonsági események három különböző módon keletkezhetnek, a keletkezési típust minden esetben rögzítik.

A törvény szerinti bejelentésnek tekinthető *az ügyfél általi közvetlen incidensbejelentés,* mely minden ügyfél részéről kötelező tevékenység. Ebben az esetben általában az intézmény által végzett elemzés értékelésére, kiegészítésére, további vizsgálati lehetőségek azonosítására helyeződik a hangsúly, egyes esetekben azonban olyan korai fázisban jelentik az incidenst, hogy az egész életciklust támogatja a GovCERT.

Feltárásnak tekinthető például a korábban részletesen tanulmányozott fenyegetettségmenedzsment során a saját monitorozói tevékenység vagy a hálózati forgalomelemzés következtében keletkező incidensek.

Jelzésként rögzítik a harmadik fél általi bejelentést. Ilyen jelzéseket megállapodás alapján vagy eseti jelleggel külföldi CERT-ek, szervezetek, vírusvédelmi megoldásokat gyártó cégek, egyéb szereplők, valamint magánszemélyek tesznek, illetve a különböző CTI- és IoC-információk alapján keletkezett incidensek is ennek tekinthetőek. Mivel nemzetközi irányban a GovCERT az elsődleges kapcsolattartó (a nemzeti CERT), ezért a nemzetközi jelzések egyik fontos belépőpontja is a szervezet.

Az utóbbi két esetben szinte mindig szükséges az incidenskezelés első és második szintjében megfogalmazott munkafolyamat lefuttatása.

Általánosságban elmondható, hogy egy állami incidens bejelentésére hat feltárás és jelzés jut, azonban a szervezet reputációjának növekedésével ez a statisztikai adat is javuló tendenciát mutat.

---

[25] 185/2015. (VII. 13.) kormányrendelet, 10. § (5).
[26] 185/2015. (VII. 13.) kormányrendelet, 11. § (1).
[27] 185/2015. (VII. 13.) kormányrendelet, 11. § (3).
[28] 2003. évi C. törvény, 92/B. §.

A biztonsági események legfontosabb bejelentési csatornája és a kapcsolattartás elsődleges formája az elektronikus levél, ezenkívül a központ telefonon, faxon és levélben is tud bejelentést fogadni, azonban a tapasztalatok alapján ezek kevésbé hatékony módjai a kapcsolattartásnak.

Az incidens bejelentésének megkönnyítése érdekében a GovCERT létrehozott és a weboldalán elérhetővé tett egy incidenst bejelentő űrlapot, valamint működik egy webes formanyomtatvány is erre a célra. Az is segíti a kapcsolattartást, hogy a hivatalos kommunikáció a ticketing rendszer segítségével, egy kizárólag erre a célra dedikált e-mail-cím használatával (cert@govcert.hu) történik.

3.1.5.4. A biztonsági események feldolgozása, elővizsgálata

Az első szintű incidenskezelés, feldolgozás és az elővizsgálat célja a biztonsági esemény lehető leggyorsabb megismerése, kezelése, gyors segítségnyújtás az ügyfelek részére, az információ-megosztás folyamatos működtetése, a rendszerbe történő gyors és folyamatos rögzítés és az, hogy az incidens a legkevesebb idő alatt a megoldás irányába mozduljon el.

A biztonsági események fogadását és feldolgozását általában a GovCERT folyamatosan, 7/24-es rendszerben működő ügyelete végzi. A munkafolyamat az alábbi lépésekből áll (azonban a napi munka során a munkafolyamatok megvalósítása nem feltétlenül ebben a sorrendben történik):

- Bejelentés fogadása.
- Validálás.
- Előzmény vizsgálata.
- Érintettség vizsgálata.
- Partnerek, érintettek azonosítása.
- Technikai adatok elemzése.
- Kockázati besorolás.
- Technikai adatbekérés összeállítása.
- Értesítés, adatbekérés.
- Intézkedési terv kiadása.
- Incidens felterjesztése.

A bejelentések fogadása a nap 24 órájában, folyamatosan történik, az esetek túlnyomó részében e-mailben. Az új bejelentéseket jelenlét alapján delegálják a kollégáknak, a munkafolyamat ezen állomását a delegált kolléga többnyire a munkaidejének végéig végrehajtja, azonban lehetőség van egyes bejelentések egymásnak történő átadására is.

A bejelentést a téves esetek kiszűrésének csökkentése érdekében *ellenőrizni, validálni szükséges.* Sor kerül a bejelentő azonosítására, melyre több módszer is rendelkezésre áll. Ilyen például az elektronikus aláírás ellenőrzése és a kapcsolattartói adatbázis segítségül hívása. Ha ez a konkrét incidenstípus alapján lehetséges, szükséges az incidens tényének ellenőrzése, valamint az adatok hitelességének vizsgálata. Például egy holnaprongálás ellenőrzése igen egyszerűen, egy elemzői célú hálózaton működő böngésző segítségével megtehető.

Az incidensek előzményvizsgálata az incidenskezelő rendszerben több szempont alapján történik. A legfontosabb összehasonlítási szempontok az intézményhez kötöttség, a típus, az IP-cím és a domainnév. Az előzményvizsgálat célja a duplikációk kiküszöbölése, azaz hogy egy incidenst csak egyszer rögzítsenek a rendszerben. Ha a rendszerben található előzmény, akkor a bejelentést csatolják, ha nem, akkor új ticket készül.

A beérkezett információk vizsgálata

Az érintettség vizsgálatára az állami és önkormányzati szervezethez tartozás azonosítása és a GovCERT hatáskörének eldöntése miatt van szükség. Ha ugyanis egy ügyfél rendszerében bekövetkezett incidenst jelentenek be, akkor arra más – ebben a tananyagban is részletezett – eljárási szabályok vonatkoznak, mint egy „nem állami" esemény bejelentése esetén.

Az állami és önkormányzati szférán kívüli incidensek koordinációjára és részletes technikai vizsgálatára a GovCERT-nek nincs felhatalmazása, az ilyen esetekben az érintett intézményhez, partnerhez, szolgáltatóhoz, esetleg a Hun-CERT-hez továbbítják az esetet kivizsgálás céljából. Ha rendelkezésre áll egyéb információ (CTI, IoC), akkor ezeket természetesen mellékelik. A vizsgálat alapja az IP-cím, a domainnév, illetve minden olyan egyéb információ, mely az esetet a konkrét intézményhez köti.

Ezt követően sor kerül az ügyfelek, a partnerek és az érintettek azonosítására, az elérhetőségek keresésére. Amennyiben nem található aktív kapcsolat a szervezettel, akkor azt fel kell venni vele egy publikusan megjelenített elérhetőségén keresztül. Amennyiben az incidens jellege megköveteli a szolgáltatóval történő kapcsolattartást, akkor a szolgáltató „who is" adatbázisában található „abuse" címére vagy az előre egyeztetett elérhetőségre küldik a megkeresést.

Ha a bejelentéssel egy időben technikai adat, bizonyíték (log állomány, e-mail-fejléc, incidensre utaló egyéb adat) is érkezik, annak vizsgálata és értékelése a lehető leghamarabb megtörténik. A különböző bizonyítékok gyorselemzésére különböző céleszközök állnak rendelkezésre.

A *kockázati besorolás* elvégzése a folyamat egyik legösszetettebb művelete, melyet csak a beérkezett adatok értékelését követően lehet elvégezni. Ha nem áll megfelelő mennyiségű információ rendelkezésre, akkor azt kell kérni a bejelentőtől, az érintettől, esetleg adatgyűjtésre is szükség lehet. Az incidens besorolására, priorizálására a hatás- és a sürgősségi vizsgálatot követően kerülhet sor. Vizsgálni kell a biztonsági esemény szervezetre, állami és önkormányzati szférára, a magyar és nemzetközi kibertérre vonatkozó jelenlegi és potenciális hatását, valamint azt, hogy mennyire gyorsan szükséges a beavatkozás a jelenlegi és a jövőbeni hatások függvényében.

A besorolás elvégzéséhez egy viszonylag egzakt módon eldönthető mátrixot kell alkalmazni, melynek segítségével gyorsan és egyszerűen hozható döntés. Ezt követően az incidens szakmai és statisztikai célú metaadatait töltik fel.

Ebben a munkafolyamati elemben is azonosíthatóak az úgynevezett *súlyos biztonsági események.* Ezek olyan speciális informatikai események, amelyeknek a bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés fenyeget az állammal vagy az érintett szervezettel szemben, alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek.[29] Ebben a speciális esetben egy erre a célra kidolgozott eljárást folytatnak le.

Első kommunikáció

A technikai adatbekérés összeállítására szükség esetén és az incidenstípushoz kötötten kerül sor: minden típus esetén léteznek olyan adatok, melyek bekérésére nagy valószínűséggel szükség lesz. Ilyen például egy adathalászat esetén az adathalász e-mail vagy a szolgáltatásmegtagadásos támadás során a különböző, ezt feltáró naplóállományok. Az eseménykezelés ilyen korai szakaszában a későbbi elemzés meggyorsítása érdekében van szükség erre a tevékenységre.

Miután az eseményről átfogó képet alakítottak ki, megtörténhet az értesítés és az adatbekérés. Az értesítéshez számos, a korábbi incidenskezelési tapasztalatok alapján készült sablon áll rendelkezésre, melyek konkrét ügyhöz igazítása minden esetben szükséges. Kitöltik az úgynevezett „adatbekérő

[29] 2013. évi L. törvény, 1. § 41a. pont.

lapot", melyre az intézmény az incidenskezelés lépéseit, megállapításait, valamint a megtett intézkedéseket tudja dokumentálni, irányított kérdések formájában. Ezt követően kiküldik az értesítést, főszabályként e-mailben. A gyakorlati tapasztalatok alapján egyes intézmények esetén telefonon is megerősítik a bejelentéseket.

Egyes incidenstípusok esetén előre definiált intézkedési tervet állítanak össze, amely az intézménynek megkönnyítheti a konkrét incidens felszámolását. Ilyenek például a weboldal rongálása (defacement), a különböző típusú robothálózatok (botnet) és a szolgáltatásmegtagadások különböző változatai (DoS, DDoS SYN Flood). Egyes dokumentumokat úgy alkotott meg a központ, hogy az abban foglalt lépéseket egy informatikában kevésbé jártas ügyfél is végre tudja hajtani. Az intézkedési terveket szükség esetén személyre kell szabni, és ha lehetséges, ezeket a GovCERT az értesítéssel együtt küldi meg az ügyfélnek.

További koordináció szükségessége esetén az eseményt felterjesztik a munkafolyamat következő fázisába. Ez nem minden esetben történik meg, azonban az állami és önkormányzati érintettségű incidensek túlnyomó többsége általában további koordinációt igényel.

3.1.5.5. A biztonsági események koordinálása

A második szintű incidenskezelés, a biztonsági események koordinálásának célja az incidens életútjának végigkísérése a megoldásig, az esemény okainak feltárása, megértése, technikai segítségnyújtás az ügyfelek részére, a szerzett tapasztalatok hasznosítása, folyamatos és kiegyensúlyozott kapcsolattartás az ügyfelekkel.

A munkafolyamat ezen egysége egy nehezen formalizálható és sablonizálható tevékenység, amely nyitottságot, kreativitást és folyamatos odafigyelést igényel. A koordinációs tevékenység az alábbi lépéseket foglalja magában, melyeket az incidens jellegétől függően akár többször, ciklikusan kell végrehajtani:

- A felelős kijelölése.
- Az incidens vizsgálata.
- Az adatok vizsgálata.
- További adatok bekérése.
- Részletes és átfogó technikai kivizsgálás.
- Folyamatos kapcsolattartás.
- Kivizsgálás értékelése.
- Intézkedési terv kiegészítése.

A folyamat a felelős kijelölésével kezdődik, mely vezetői tevékenység. Incidensenként kijelölnek egy ügygazdát. A delegálás elsősorban az ügytípustól függ, az incidens kezelője általában komoly tapasztalattal rendelkezik az adott típusú incidenssel kapcsolatban. A koordinátor felelős a folyamatos kapcsolattartásért, a technikai adatok elemzéséért, a metaadatok karbantartásáért, a dokumentáció elkészítéséért.

Az ügy kezelőjének első feladata az incidens részletes áttekintése. Mivel minden kommunikációs lépést rögzítenek az incidenskezelő rendszerben, minden egy helyen található, ezért ezt viszonylag egyszerűen meg lehet tenni, ám annál nagyobb precizitást és figyelmet kíván, az apró részleteknek ugyanis később komoly jelentősége lehet. A meglévő adatok körének behatárolására és leltározására is szükség van, a későbbi elemzés megkönnyítésének érdekében.

Ezenkívül, mivel az első kapcsolatfelvétel már megtörtént, az intézmény válasza és egyéb további információk is rendelkezésre állhatnak. Ebben az esetben az incidens metaadatainak frissítésére is szükség lehet. A korábban és újonnan beérkezett adatok vizsgálatának hasznosságát, a további adatbekérés szükségességét is meg kell állapítani.

Ezt követően kerülhet sor a beérkezett adatok elemzésére, melyhez speciális elemző eszközök állnak rendelkezésre. A leggyakrabban beérkezett technikai adatok a naplóállományok, az e-mail-információk és a nyers hálózati forgalom. Az adatok beérkezését követően a prioritás szerint a lehető leghamarabb el kell végezni az adatok elemzését és értékelését.

Az incidens okának, bekövetkezésének teljesebb feltárása érdekében további adatok bekérésére is sor kerülhet. Ebben az esetben folyamatos és együttműködő kommunikáció szükséges az ügyféllel, az adatgazdával a potenciális adatok körének meghatározása érdekében.

A GovCERT az érintett intézmény bevonására törekszik, ezért a folyamatos kapcsolattartás elkerülhetetlen a jó minőségű incidenskezeléshez. Szükség esetén, kérésre az ügygazda státuszriportot is készít az ügyfélnek, illetve egyéb szereplőknek. Az incidens kezelése során emellett folyamatos tevékenység a dokumentálás, valamint a metaadatok frissítése és aktualizálása, szükség esetén a besorolás ismételt elvégzése is. Továbbá az incidenskezelés során keletkezett újabb szálak megnyitása esetén az első szintű incidenskezelésben felsorolt tevékenységeket is szükség szerint újra el kell végezni.

A kivizsgálás végső értékelésére a potenciálisan és szóba jöhetően begyűjthető adatok bekérését, az adatbekérés lezárását és az összes technikai információ elemzését követően kerülhet sor. Ebben a részfolyamatban kerül sor a találatok és a megállapítások strukturált formában történő rögzítésére.

Az incidens jellegétől, illetve az értékelés eredményétől függően szükség lehet az intézkedési terv kiegészítésére, ha a korábban kiadott dokumentum nem támogatja maradéktalanul a problémamegoldást. Egyes esetekben személyre szabott javaslatok megállapítása történhet.

3.1.5.6. A biztonsági események részletes technikai vizsgálata

A harmadik szintű incidenskezelés célja az incidensek okának részletes és mély elemzése, az esemény okainak feltárása, konkrét, személyre szabott megoldási terv készítése, megelőzési javaslatok kidolgozása. A munkafolyamatban részt vevő személyeket erre a feladatra jelölik ki, nagy tapasztalattal rendelkeznek mind az első, mind a második szintű incidenskezelésben, valamint az incidensek technikai kivizsgálásában. Az incidenskezelési folyamat ezen része is igazi csapatmunka: több kolléga párhuzamosan dolgozza fel, elemzi és értékeli a beérkezett információkat, valamint folyamatosan dokumentálja a megállapításokat, az eredményeket.

A biztonsági események részletes technikai vizsgálata nem feltétlenül része a teljes incidenskezelésnek. Abban az esetben indulhat technikai vizsgálat, ha az incidens besorolása, az incidens jellege, a technikai adatok minősége vagy mennyisége ezt indokolja. Minden esetben indul vizsgálat az ügyfél kérésére, vezetői döntés, valamint súlyos biztonsági esemény esetén. A kivizsgálás csak a felek, tehát az ügyfél és a központ szoros együttműködésével, közös akarattal végezhető.

Súlyos biztonsági incidens esetén minden esetben szükséges technikai kivizsgálás. Ebben az esetben az incidenskezelés kezdeti fázisába bekapcsolódik a technikai kivizsgáló csapat. Szükség esetén, az incidenskezelés korai szakaszában sor kerülhet helyszíni jelenlét biztosítására is. A súlyos biztonsági esemény szerinti eljárást kizárólag vezető rendelheti el.

Az első lépés a beérkezett adatok összegzése, részletes leltár készítése, valamint a korábbi elemzések áttekintése. Ezt követően az esetek döntő többségében további adatok bekérése szükséges, mely sok esetben igen nagy mennyiségű és érzékeny besorolású. Az adatbekérés az egyes vizsgálatok elvégését követően, azok eredményére tekintettel többször is megtörténhet.

A viszonyok, a hatáskörök tisztázása érdekében az ügyfél kérésére megbízólevél készül, mely tartalmazza az incidens számát, tárgyát, a jogalapot – amely az állami és önkormányzati incidensek esetében a 185/2015. számú kormányrendelet 10. § (2)–(3) bekezdései és a 12. § (2) bekezdése –, valamint az incidenssel megbízott személyek nevét, továbbá egyéb, az azonosításra alkalmas adatokat.

A technikai kivizsgálás sok időt és munkát igénylő folyamat, ezért a párhuzamosságok és a felesleges vizsgálatok elkerülése érdekében szükség van a vizsgálat tárgyának azonosítására, ami lényeges és megkerülhetetlen momentum.

A GovCERT – az incidens körülményeitől függően – általában a személyes egyeztetést javasolja. A találkozó alatt az összes lényeges kérdés tisztázható. A legfontosabb feladatok az esemény, a probléma és az eddigi intézkedések megismerése, a rendszerismeret, a vizsgálatra alkalmas eszközök és adatok azonosítása, a lehetőségek számbavétele. Egy személyes találkozón igény szerint röviden ismertetik a központ rendelkezésre álló elemzési képességeit, lehetőségeit.

A leggyakoribb vizsgálati módszerek a különböző típusú naplóállományok elemzése, a számítógépes nyomelemzés és a káros kódok, más néven malware-ek elemzése. Az adatok és rendszerek biztonsága érdekében mindegyik vizsgálatot egy erre a célra létrehozott, zárt, szeparált hálózaton, dedikált eszközök használatával kell elvégezni.

A naplóállományok elemzésének célja a rendszerekben bekövetkezett események okának és következményének feltárása, a támadó és a támadási módszer azonosítása, az esetleges konfigurációs hiányosságok feltárása. Mivel rengeteg típusú naplóállomány létezik, ezért minden esetben a logállományok megértése az első mozzanat. A naplóállományok feldolgozására speciális logelemző rendszerek állnak rendelkezésre.

A számítógépes nyomelemzés (forensics) tevékenység célja a bejelentésben foglaltak ellenőrzése, valamint a további adatgyűjtés. A legfontosabb elemzésre alkalmas információk a fájlrendszer, valamint annak változása, a metaadatok, a törölt állományok vizsgálata, a Windows Registry kulcsok, a böngésző és az e-mail-kliens adatai, valamint a rendszerben megtalálható kártevőkutatás.

A káros kód elemzésének célja a rendszerbe került, nem legális tevékenységet végző programok működésének megértése. Erre több módszer is létezik, azonban összefoglaló jelleggel kijelenthető, hogy ezek mindegyikének alkalmazása komoly szakmai tudást és tapasztalatot igényel. A *statikus analízis* a káros kód futtatása nélkül, a *dinamikus analízis* annak futtatásával végez vizsgálatot. A viselkedés alapú analízis során a céleszköz, a hálózati analízis során a kapcsolódó hálózatok és a káros kód működésének megfigyelése történik. Az automatikus analízis ennek a négy módszernek az ötvözete is lehet.

A vizsgálatok alapján talált különböző indikátorokat (IoC) és támadási vektorokat a GovCERT megosztja a hazai és a nemzetközi partnerekkel, valamint a további biztonsági események azonosítása érdekében hálózati forgalomelemzésre is lehetőség van.

A *dokumentálás* a technikai kivizsgálás elkerülhetetlen és fontos eleme. Minden ilyen vizsgálatról részletes jelentés készül, melyet az incidensben érintett intézménynek továbbítanak. Az intézmény kérése esetén – az elemzés addigi állásának rögzítése céljából – lehetőség van státuszriport kiadására is. Az elemzéshez hasonlóan a dokumentálás is több kolléga együttes munkája. A jelentés készítésének célja az intézmény tájékoztatása, a biztonság erősítése és a tapasztalatok átadása.

A jelentés felépítése az esetek többségében egységes: minden esetben egy–másfél oldalas vezetői összefoglalóval kezdődik, majd a bevezetéssel, az incidens körülményeinek leírásával folytatódik. Ezt követi az átadott adatok körének leírása, valamint a módszertan rövid ismertetése. A jelentés leghosszabb része a különböző vizsgálatok, elemzések leírása, valamint az eredmények megállapítása, amelyet általában gazdagon illusztrálnak technikai adatokkal és ábrákkal. A jelentést a megállapítások összefoglalása, valamint a javaslatok zárják, az összterjedelem általában 10 és 20 oldal közötti.

3.1.5.7. A biztonsági események lezárása

A biztonsági események aktív szakaszának utolsó mozzanata az incidens lezárása, melynek célja a biztonsági esemény kezelésének vizsgálata, az elért eredmények és egyéb intézkedések értékelése. A műveletet általában az ügygazda végzi az incidenskezelő rendszer aktív használatával és segítségével.

Sor kerül az incidens során beérkezett és keletkezett információk, valamint elemzések áttekintésére, a visszaküldött adatkérő lap vizsgálatára. A megtett intézkedések ellenőrzése is fontos lehet, amit elsősorban a leírtak alapján, empirikusan vagy technikai vizsgálattal végeznek. Az intézményt és az összes résztvevőt (például szolgáltatót, bejelentőt) minden esetben – manuálisan vagy

automatikusan – tájékoztatnak. A végleges lezárás előtt az incidenst minden esetben áttekinti a vezető is, és döntésének megfelelően jóváhagyja vagy visszautasítja a lezárást.

A munkafolyamat végén az incidenskezelés eredményétől, illetve a megoldástól függően öt különböző lezárási mód alkalmazható.

Az incidens *teljes körű megoldásáról* akkor beszélünk, ha az incidens felszámolása sikeresen megtörtént, a megtett intézkedések ellenőrzése sikeres, az intézmény eljárása megfelelő volt, a javaslatokat beépítették, valamint megtörtént a megelőző intézkedések alkalmazása is.

A biztonsági esemény *korlátozott (nem teljes) megoldása* az incidens tüneti okainak megszűnését jelenti, mivel olyan körülmény van jelen a rendszerben, amely nem teszi lehetővé a teljes körű megoldást. Ebben az esetben várható az incidens újranyílása, és a lezárás csak az intézmény részletes indoklása esetén lehetséges.

Ha a hivatalos csatornákon *sikertelen a kapcsolatfelvétel az intézménnyel,* akkor az incidens ezen okból szintén lezárható. A központ minden esetben több csatornán (általában e-mailben és telefonon) is megkísérli felvenni a kapcsolatot ügyfelével, ezt minimum harminc napig, heti egy alkalommal kísérli meg az ügygazda.

Ha az intézmény *a törvényi kötelezettségének több felszólítás ellenére sem tesz eleget,* a biztonsági esemény az együttműködés hiánya miatt lezárható. Ebben az esetben a kommunikáció folyamatos, de az intézmény nem törekszik a megoldásra .

A lezárás *egyéb okból* is elképzelhető: ilyenek lehetnek a szervezet jogutód nélküli megszűnése, a szerver lekapcsolása vagy a weboldal megszűnése.

A lezárás speciális esetei esetén, tehát sikertelen kapcsolatfelvétel és az együttműködés hiánya miatt a biztonsági esemény kezelése hatósági szakaszba kerül. Ebben az esetben a központ hatósági eljárást kezdeményez a Nemzeti Elektronikus Információbiztonság Hatóságnál. Megtörténik az adatok átadása, a megtett intézkedések tételes felsorolása, szükség esetén személyes egyeztetésre is sor kerül.

A hatósági eljárás egy végzés kibocsátásával kezdődik, melyet papír alapon juttatnak el a szervezet első számú vezetője részére, határidő megjelölésével. A végzés tartalma megegyezik az incidenskezelésben megfogalmazott tartalmakkal, és konstruktív együttműködésre szólítja fel az intézményt. Az eljárás alapja a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény. Az eljárás végzéssel zárul. Sikertelenség esetén a hatóságnak jogában áll felügyelőbiztost kirendelni.

Az incidens tényleges lezárása az incidenskezelő rendszerben történik. Minden esetben dokumentálják a lezárás körülményeit, valamint megtörténik a kapcsolódó metaadatok frissítése is. A GovCERT által végzett *post mortem* vizsgálat legfontosabb célja az incidenskezelés hatékonyságának értékelése, a szerzett tapasztalatok összegzése és tudásbázisba rögzítése, szükség esetén az intézkedési tervek kiegészítése, valamint új intézkedési terv kidolgozása.

3.1.5.8. A biztonsági események utóélete

Abban az esetben, ha az incidenst lezárták, azonban az esemény ugyanazon okból ismét bekövetkezik vagy a megoldás mégsem járt a várt sikerrel, a jegy (ticket) újból aktív státuszba kerülhet, az incidenskezelés pedig koordinációs szakaszban folytatódik.

Az incidensekben keletkezett technikai adatokat a lezárást követően 60 nappal véglegesen törlik, az incidenskezelő rendszerben tárolt metaadatok, valamint a kommunikáció azonban hosszú ideig elérhető maradnak. Ennek statisztikai, valamint nyomon követhetőségi okai vannak.

A biztonsági eseményekről a tapasztalatok átadása miatt kizárólag teljesen anonim összefoglalók készíthetőek, és ezeket is csak zárt körben osztják meg. A megosztás elsődleges címzettje a GovCERT ügyfélköre, azonban nagyobb jelentőségű, nemzetközi vetületű vagy nemzetközi érdeklődésre számot tartó események esetén a külföldi partnerek tájékoztatása is megtörténik.

Az incidensek kezelése során keletkezett metaadatokat a GovCERT szintén anonim, mások által visszakövethetetlen módon, a különböző termékekben rendszeres időközönként igyekszik megjeleníteni. A cél az, hogy a felhasználó egy átfogó képet szerezzen az állami és önkormányzati szféra információbiztonsági helyzetéről, megismerhesse az aktuális trendeket, problémákat.

3.1.5.9. Gyakorlati tapasztalatok

Az intézmények incidensekről tett bejelentési hajlandósága továbbra is elég alacsony, azonban biztató adat a bejelentések számának és arányának folyamatos növekedése.

Mivel a szervezetek többsége nem rendelkezik Incidenskezelő csapattal (IRT), valamint általában csak munkaidőben és akkor is csak korlátozottan foglalkoznak ezzel a tevékenységgel, ezért a reagálási idő elnyúlik. (Az utóbbi időben azonban ezen a területen is történnek pozitív változások.) Ezen okok miatt az intézmények a kártékony kódok jelenlétét általában későn észlelik és jelzik, ezért a biztonsági események kapcsán csak késve, az aktív tevékenység lezajlását követően tesznek intézkedéseket.

A technikai személyzet sok esetben tapasztalatlan és képzetlen az incidenskezelés és az információbiztonság terén, mivel a szervezetek többsége az üzemeltetésre helyezi a hangsúlyt. Sok esetben ugyanaz a szervezeti egység foglalkozik az üzemeltetéssel és a biztonsággal. Ennek káros következményeivel gyakran szembesül a központ. Az ok általában a munkaerő- és a forráshiány, a vezetői akarat, valamint az információ hiánya.

Az előzőekből fakadóan kijelenthető, hogy sok szervezetnél alacsony az informatikai biztonság szintje, a munkavállalók információbiztonsági tudatossága is gyenge, hiszen sok incidens felhasználói gondatlanság miatt következik be. Ezekkel szemben a legkönnyebben és legolcsóbban tudatosító kampányokkal harcolhatunk.

Sok szervezetnek adatvédelmi és adatkezelési aggályai vannak az incidenskezeléssel, azt gondolják, hogy a saját rendszerükben bekövetkezett incidensek kizárólag szervezeten belüli rendezést igényelnek. Ez a vélekedés általában a központ és a jogszabályok nem teljes körű ismerete következtében alakul ki.

3.1.5.10. Intézkedési terv az NKI-val közös incidenskezelésre

A biztonsági eseményeket javasolt folyamatosan, a kezelés lehető legkorábbi szakaszában bejelenteni, mert ezzel lehet biztosítani, hogy a GovCERT a lehető legtöbb segítséget tudja nyújtani, a leghasznosabb tapasztalatokat tudja átadni az intézménynek. A bejelentésben feltétlenül fel kell tüntetni az incidenst kiváltó tüneteket, az egyéb körülményeket, az eddig azonosított eseményeket, az elemzett adatokat, az érintett rendszereket, valamint a releváns technikai adatokat.

Javasolt személyes találkozók, megbeszélések szervezése. A központ mindig nyitott a hasonló eseményeken való aktív részvételre, szükség esetén házigazdai szerepet is vállal. Az incidenskezelés és az együttműködés bizalmi kérdés is, ezért törekedni kell a személyes ismertségre, a folyamatos kommunikációra és tapasztalatcserére. A 2017-ben induló incidenskezelési megbízotti képzés és számos konferencián történő megjelenés erre megfelelő lehetőséget teremt.

A kommunikáció zavartalanná tételéhez a kapcsolati információk folyamatos frissítése javasolt: a kijelölt kapcsolati személyek, az egyéb szervezeti változások bejelentése megkönnyíti és lerövidíti a kapcsolatfelvételt.

Incidenstípusonként eltérő azon adatok köre, amelyek elemzésével hasznos információkhoz lehet jutni és amelyek előremozdítják az incidenskezelést. Természetesen nem ugyanazokra az adatokra lesz szükség egy szolgáltatás-megtagadásos támadással, egy célzott adathalászattal vagy egy zsarolóvírussal kapcsolatos incidens kezelésekor.

Az incidenskezeléshez általában az alábbi adatok szükségesek:

- Az eszköz memóriaképe az első helyen található, mert mind közül ez a legsérülékenyebb adat. Például egy munkaállomás kikapcsolását követően az adatok nem állíthatóak helyre, pedig egy káros kód fertőzése esetén ez az egyik leghasznosabb információforrás.
- Röviden érdemes beszámolni a megtett intézkedésekről, hogy azonosítani lehessen az incidenskezelés jelenlegi státuszát. A beszámolóból sok esetben az is kiderül, hogy milyen elemzési lehetőségek hiúsulnak meg.
- A rendszerek rövid leírására az elemzésre alkalmas adatok számbavétele miatt van szükség. Érdemes feltüntetni a különböző naplózási pontokat, a határvédelmeket, a végpontvédelmet.
- A teljes körű elemzéshez a káros tartalmú e-mail-üzenetek egésze szükséges. A levelezőkliensek többsége alkalmas az üzenetek kimentésére, például msg vagy eml formátumban, melyek jóval több információt hordoznak incidenskezelési szempontból.
- A naplóállományok ismertetésekor a logolási pontok megismerésén túl fontos lehet a logolási házirend, valamint az elérhető naplófájlok típusa. Incidenstípusonként igen eltérőek az elemzéshez szükséges naplóállományok, azonban az kijelenthető, hogy a legfontosabbak a tűzfal, a proxy és a különböző alkalmazás- és hibalogok, valamint az érintett rendszerek azonosításához szükséges egyéb információk.
- Az adathordozók, valamint a lemezkép vizsgálatával rengeteg információhoz juthatunk, azonban itt található a legtöbb bizalmas adat is. A káros kód kutatásának másik legfontosabb módja egy klienseszköz vizsgálata.

A GovCERT támogatása érdekében javasolt a segítségnyújtás típusát is az incidens bejelentésével együtt definiálni, mert ez segíthet az ügygazdának az incidens kezelése során arra a területre összpontosítani, mely a legnagyobb relevanciával bír az intézmény számára.

3.1.5.11. Incidenskezelés a gyakorlatban

A továbbiakban ismertetünk három konkrét incidenst, illetve kampányt, azok körülményeit, az elemzések típusait, eredményeit, valamint a tapasztalatokat és a megelőzésre vonatkozó tanácsokat. A három incidens közös jellemzője, hogy az esemény egy elektronikus levél érkezésével kezdődik, azonban a támadók célja mindhárom esetben más, és az incidensek kockázati besorolása is különbözik.

Célzott adathalászat

Ez a támadástípus abban különbözik az egyszerű adathalászattól, hogy célzottan egy intézmény, intézménycsoport vagy szektor ellen irányul. A támadó célja, hogy a felhasználót megtévesztve felhasználói vagy személyes adatot szerezzen. Az ilyen jellegű incidensek általában közepes kockázati besorolásúak, de a támadás sikerességétől és jellegétől függően ez változhat.

A támadók általában összegyűjtik az interneten fellelhető, a szervezethez köthető elektronikus levélcímeket, majd ezekre megtévesztés céljából leveleket küldenek, amelyek minősége és kidolgozottsága erősen eltérő. Általában hamisított feladót használnak, sok esetben szervezeten belülinek tűnő levélként érkezik a megtévesztő tartalom. Ezek miatt a forrás azonosítása igen nehézkes, időigényes, sok esetben sikertelen.

Évente több tíz ilyen és ehhez hasonló incidens bejelentés történik a GovCERT-hez, általában hullámokban, egyszerre több intézményhez érkeznek az e-mailek, amelyekben az esetek döntő többségében egy megtévesztő weboldalra hivatkozó URL található, valamilyen figyelmeztető – például jelszóváltoztatásra felhívó – üzenettel. Minden esetben adatbekérés történik az intézményektől, általában e-mail-adatok és proxylogok vizsgálata válik szükségessé.

Az elektronikus levélben található adatok elemzésének célja az incidens indikátorainak (feladó e-mail-címe, domain, URL) és a támadási vektorok (támadás pontos típusa) azonosítása, mely alapján hálózati forgalomelemzés és -tiltás is kezdeményezhető. A proxy naplóállományok bekérésének célja az érintett munkaállomások, valamint a sikeres adathalászat azonosítása. Az információkat elemezve és értékelve kerülhet sor a további érintettek azonosítására.

A megtévesztő weboldalak minősége igen eltérő. Akadnak primitív adathalász kísérletek, de sokszor találkozni egy bank, webes levelezőkliens vagy egy közösségi oldal igen jól sikerült másolatával is, amelyhez gyakran megtévesztő domaint használnak. A megszerezni kívánt adatok köréből lehet következtetni a támadók céljára is. A feltárt adathalász oldalakat több mint tíz releváns, az adathalászat megakadályozására létrehozott felületen is bejelentik, ennek eredményeképp például a böngészők rendkívül gyorsan – egyes esetekben perceken belül – figyelmezető üzeneteket jelenítenek meg az oldal meglátogatásakor.

Egy-egy kiterjedtebb kampány esetén a nemzetközi partnerek tájékoztatása, valamint az indikátorok megosztása is megtörténik. A nemzetközi adatmegosztásból származó információk alapján több alkalommal tárható fel adathalász tevékenység a kormányzati szférában.

A felhasználói tudatosság növelése az első és legfontosabb védvonal az ilyen jellegű támadásokkal szemben: ismeretlen feladótól érkező gyanús csatolmánnyal, esetleg hivatkozással ellátott leveleket – amennyiben ez lehetséges – javasolt azonnal karanténba helyezni, majd megvizsgálni. A belső feladóval érkező külső levelek kiszűrésére az esetek többségében létezik konfigurációs beállítás, emellett javasolt a kéretlen leveleket szűrő és az URL-eket is vizsgáló végpontvédelmi rendszer vírusdefiníciós adatbázisának folyamatos frissítése.

Zsarolóvírus

A zsarolóvírus a káros kódok egy speciális típusa, a célja a felhasználó által elérhető, előre meghatározott formátumú adatok elérhetetlenné tétele kriptográfiai algoritmusokkal vagy egyéb módszerrel. Ezt követően a zsaroló egy üzenet segítségével általában „váltságdíjat" követel az adatok visszaállításáért. A támadók csak előre definiált formátumú (általában multimédiás és dokumentum jellegű) adatokat titkosítanak, mivel a zsarolóüzenet megjelenítéséhez szükséges a működő operációs rendszer.

A zsarolóvírusok kockázati besorolása leginkább a hatásuktól függ. Ha egy káros kód egy olyan intézményhez érkezik, ahol hatékony védelemmel és felhasználói tudatossággal megakadályozzák annak futtatását, akkor alacsony, ha azonban olyan rendszerben fut le sikeresen a malware, ahol az adatok nem visszaállíthatóak, magas vagy kritikus besorolást is kaphat.

2016-ban 10 másodpercenként egy lakossági ügyfél és 40 másodpercenként egy vállalati ügyfél szenvedett zsarolóvírusos támadást; a jelenlegi ismeretek szerint több mint 60 víruscsalád 54 000 variánsa kering a nemzetközi kibertérben.[30]

A *ransomware*-ek népszerűségének oka az, hogy elérhetőek úgynevezett *bulderek,* melyekkel igen könnyen lehet létrehozni saját variánst. Ezenkívül a káros kód terjesztése szolgáltatásként is elérhető, valamint a fizetés anonimitása (bitcoin) viszonylagos lenyomozhatatlanságot jelent az elkövetőknek.

A víruscsaládok fejlődése folyamatos, ezért ez egyre inkább világméretű problémává válik. A lakossági és a kisvállalati szektorból a nagyvállalatokra terelődik a támadások fókusza, mivel ott egyetlen sikeres támadással is óriási profit érhető el. A folyamatos fejlődés a támadóktól is nagy erőforrásokat és befektetéseket igényel, ennek ellenére ez a kiberbűnözési ág jelenleg igen nagy bevételt termel.

A zsarolóvírusok a leggyakrabban az előző példában bemutatott módon: e-mailben, csatolmány vagy URL segítségével, a böngésző vagy a dokumentumkezelő sérülékenységének kihasználásával, tehát felhasználói interakció segítségével terjednek.

[30] Garnaeva, Maria – Sinitsyn, Fedor – Namestnikov,Yury – Makrushin, Denis – Liskin, Alexander (2016), 10.

Ezek mellett új támadási formák is megjelennek, melyek a távoliasztal-szolgáltatások (RDP) gyengeségeit vagy hibás konfigurációját használják ki, és így jutnak be a felhasználó rendszerébe. Ezt követően a szolgáltatást használva képesek kifejteni a káros tevékenységet. Egyre inkább elterjednek azok a módszerek, melyekben a támadók nem titkosítanak, hanem jelszavas archívokat használnak. Ennek az az oka, hogy így a káros tevékenység nem igényel semmilyen telepítést, az alkalmazás rendelkezésre áll a rendszerben, és a károkozás, a fájlok elérhetetlenné tétele így is megtörténik.

Egy a GovCERT-hez érkezett bejelentés szerint egy állami intézmény szerverén tárolt állományokat titkosítottak, a lemezekről biztonsági másolat nem készült. A támadók zsarolólevelet (*ransomnote*) helyeztek el minden olyan mappában, ahol adattitkosítás történt. A központ az incidens kivizsgálása érdekében, valamint az adatok esetleges visszaállítása miatt bekérte a szerver lemezképét.

Ennek felhasználásával és elemzésével a zsarolóvírus típusát – a *ransomnote* üzenet, a kiterjesztés formátuma, valamint a registry bejegyzések alapján –azonosították, azonban a visszafejtés sikertelenül zárult, mert bár a víruscsalád ismert volt, de a támadók egy új variánst használtak. A korábbi verzió ismert hibáját kihasználva visszaállíthatóak voltak a titkosított fájlok a titkosítási kulcs ismerete nélkül is, azonban az ebben a támadásban használt variáns esetén ezt a hibát kijavították.

Az adatok elemzésekor kiderült, hogy a támadás RDP-n keresztül történt, valamint az is látszott, hogy a bejelentkezés után a támadó a böngészőből töltötte le a káros kódot, tehát a víruson kívül semmilyen speciális eszközt nem használt.

A támadások ellen a legjobb védekezés – a felhasználói tudatosításon, valamint a nem használt protokollok tiltásán túl – az, ha az adatokat nem a munkaállomásokon, hanem adatkörökben tárolják, emellett az ilyen jellegű adatvesztésnek folyamatos, ütemezett biztonsági mentés készítésével is elejét lehet venni.

Összetett célzott támadás

A célzott támadást vagy APT-t (*advanced persistent threat*) államilag támogatott, kiberkémkedésre vagy ipari kémkedésre szakosodott csoportok használják. A támadások hasonló összetettségűek, azonban a céljaik eltérnek egymástól. A kiberkémkedést politikai célok hívták életre, általában védelmi és geopolitikai kérdésekben történik adatszivárogtatás, míg az ipari kémkedés célja üzleti titkok és érzékeny adatbázisok megszerzése. Az ilyen jellegű incidensek a sikerességüktől függően változó kockázati besorolást kapnak, de az összességében elmondható, hogy a besorolás a támadás összetettsége miatt általában magas szintet ér el.

Az elemzések szerint a támadások mögött profi szereplők, teljes és jól felkészült fejlesztői és üzemeltetői csapat áll. A támadásra használt káros kódokat folyamatosan javítják, frissítik, az esetleges hibákat hamar befoltozzák. Egy moduláris szerkezetű keretrendszert használnak, mely számos támadási és adatszerzési technikát ismer. A forráskódokban jól ismert függvénykönyvtárak szerepelnek, ennek elsődleges oka valószínűleg a letagadhatóság.

A támadók az esetek többségében ügynevezett *0-day* sérülékenységeket használnak. Ezek olyan biztonsági rések, melyek a nagyközönség és valószínűleg a gyártó számára sem ismertek, így javítás sem érhető még el ezekre. Egy ilyen sérülékenység felszínre kerülését követően a támadók egy következőt vesznek használatba.

Ilyen esetben általában több csatornán érkezik a rendkívül szofisztikált támadás, azonban az általában kiberkémkedésre és kiberhírszerzésre használt módszer is ismeri a rendszerek leggyengébb pontját, a „humán interfészt”, azaz az emberi tényezőt.

Az első lépés olyan célzott levelek küldése az intézménynek, vállalatnak, amely URL-t vagy fertőzött dokumentumot tartalmaz, tehát indításához felhasználói interakció is szükséges. Ismert egy *watering hole* nevű támadástípus, melyben vagy a célpontok által potenciálisan látogatott legitim oldalakba injektálnak káros tartalmat, vagy létrehoznak egy olyat, melyet nagy valószínűséggel meglátogatnak.

A támadás következő lépése a profilozás, az adatösszegzés, amire azért van szükség, hogy csak a támadók célcsoportjába tartozó áldozathoz jusson el a káros kód. Ha a célpontot azonosították, következik az *exploit kit* használata, valamint a káros kód telepítése. A rendszerbe jutást követően, egy újabb sérülékenység kihasználásával történik a jogosultsági szint emelése, amelyet követően a támadó teljesen át tudja venni az irányítást az áldozat rendszerében. Az adatszivárogtatás általában titkosított csatornán, kisméretű csomagokban, lassan, türelmesen, több IP és domain használatával történik.

Az ilyen incidensek vizsgálatához nagy mennyiségű technikai adat: több munkaállomás, több szerver és egyéb eszköz adatai, lemezképek, logadatok szükségesek. Szofisztikáltsága miatt a támadás azonosítása és bizonyítása sem egyszerű. A káros kódok elemzését az obfuszkáció – a kód nehezen elemezhetővé tétele –, a C&C és egyéb kommunikáció azonosítását a gyakran változó indikátorok, valamint a technikák gyakori cserélése nehezíti.

Ebben az esetben az egyik leghatékonyabb védekezés szintén a felhasználói tudatosítás, a rendszerek folyamatos naprakészen tartása, valamint a szükségtelen szolgáltatások, szolgáltatáselemek használatának kiszűrése, mellőzése. Az ilyen támadásokat hatékonyan és nagy százalékkal kezelni tudó megoldások (IDS, IPS, anti-APT-eszközök) igen költséges beruházást igényelnek, de így sem nyújtanak biztos védelmet a támadások ellen.

3.1.6. Sérülékenységvizsgálat

A sérülékenységvizsgálat az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárására irányuló tervezett és szervezett tevékenység.[31] Az Ibtv. alapján 3-as biztonsági osztályba sorolt új elektronikus információs rendszer esetén kötelező sérülékenységvizsgálatot végezni, ami a GovCERT ügyfelei számára ingyenes szolgáltatás.

A vizsgálat célja továbbá a feltárt hibák elhárítására részletes megoldási javaslatok kidolgozása, az elektronikus információs rendszerek, rendszerelemek védelmének és biztonságának megerősítése érdekében.[32]

Fontos megjegyezni, hogy az érintett rendszerek különböző irányokból történő kompromittálhatóságának mérése a vizsgálat ideje alatti állapotra vonatkozik, tehát a rendszerben történő változtatással más sérülékenységek, biztonsági rések is keletkezhetnek, és ekkor új vizsgálatra lehet szükség.

A nemzetbiztonsági védelem alá eső szervek elektronikus információs rendszereinek, az állami és önkormányzati szervek európai létfontosságú rendszerelemmé vagy nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt elektronikus információs rendszerei, valamint a zárt célú elektronikus információs rendszerek sérülékenységvizsgálatát a Kormányzati Eseménykezelő Központ végzi. Az elektronikus információbiztonságról szóló törvény alapján továbbá a központ jogosult állami szervként a sérülékenységvizsgálat lefolytatására.[33]

A sérülékenységvizsgálat tárgya az adatok és az információk kezelésére használt elektronikus információs rendszerek, rendszerelemek, eszközök, eljárások és kapcsolódó folyamatok vizsgálata, valamint az ezeket kezelő személyek általános informatikai felkészültségének, az érintett szervezetnél használt informatikai és információbiztonsági előírások, szabályok betartásának vizsgálata.[34]

[31] 2013. évi L. törvény, 1. § 40. pont.
[32] 2013. évi L. törvény, 15. § (1) bekezdés.
[33] 185/2015. (VII. 13.) kormányrendelet, 14. § (1) bekezdés.
[34] 2013. évi L. törvény, 15. § (2) bekezdés.

3.1.6.1. Sérülékenységvizsgálati tevékenység

A sérülékenységvizsgálatot célszoftverek segítségével végzik, amelyek a biztonsági vizsgálati eljárás során kifejezetten a sérülékenységvizsgálat egyes fázisainak végrehajtására kifejlesztett alkalmazások.[35] A programok beállítása, valamint a vizsgálati eljárás mélysége alapján *megkülönböztetünk automatizált és manuális vizsgálatot.*

Az automatizált informatikai biztonsági vizsgálat olyan biztonsági vizsgálati eljárás, amelynek során az érintett szervezet informatikai rendszerének sérülékenységeit kimondottan célszoftverek segítségével térképezik fel.[36]

A kézi vagy manuális informatikai biztonsági vizsgálat olyan biztonsági vizsgálati eljárás, amelynek során az érintett szervezet informatikai rendszerének sérülékenységeit a vizsgálatot végző személy által egyedileg, manuálisan összeállított lekérdezések alkalmazásával vizsgálják.[37]

Irányultságok

A sérülékenységvizsgálat során az eljárást megalapozó dokumentációban (a projektalapító dokumentumban) meghatározottak szerint sor kerül külső informatikai biztonsági vizsgálatra, webes vizsgálatra, belső informatikai biztonsági vizsgálatra, illetve a vezeték nélküli hálózat informatikai biztonsági vizsgálatára.

A belső informatikai biztonsági vizsgálat olyan vizsgálati eljárás, amelynek során az érintett szervezet informatikai rendszerének sérülékenységvizsgálata a belső hálózati végpontról – a megrendelő aktív támogatásával – közvetlenül történik.[38]

Az ilyen irányultságú vizsgálatok első fázisa a regisztrált felhasználói jogosultság nélküli felderítés. A második fázisban (a személyi, technikai, logisztikai feltételek teljesülése esetén) a jogosultsággal végzett vizsgálatok következnek, beleértve a különböző speciális vizsgálati lehetőségeket. Eszköz- és szoftverkonfigurációs ellenőrzések során az érintett rendszerelemek beállításainak megfeleltetése történik a szakmai elvárások és irányelvek teljesülése érdekében. Vastagkliens architektúrában a saját fejlesztésű kliens–szerver alkalmazások vizsgálata zajlik le. A forráskód-analízist a Microsoft által meghatározott Security Development Lifecycle (SDL) módszertan implementációs fázisa szerint végzi a GovCERT.

A külső vizsgálat az informatikai rendszer internet felőli, külső sérülékenységvizsgálata, amelynek során az interneten fellelhető, nyilvános adatbázisokban való szabad keresésre, a célzott információgyűjtésre, valamint az elérhető számítógépek szolgáltatásainak, sebezhetőségének feltérképezésére kerülhet sor.[39]

A külső vizsgálat általában interneten fellelhető, publikus adatbázisokban való releváns adatok keresésére és gyűjtésére, a hálózati struktúráról, a telepített hardver- és szoftverelemekről való célzott információgyűjtésre, a célszegmensben elérhető számítógépek, eszközök operációs rendszerének, szolgáltatásainak, azok verziószámának és sebezhetőségeinek feltérképezésére, a határvédelmi eszközök és sebezhetőségeinek feltérképezésére és a szolgáltatás megtagadására vagy terheléses analízisre irányul.

A webes vizsgálat egy olyan eljárás, amelynek során automatizált és kézi vizsgálatok útján tárják fel a webes alkalmazások sérülékenységeit.[40] A webes alkalmazások sérülékenységvizsgálata az OWASP Testing Guide v4 ajánlásai alapján történik. A vizsgálatok az automatizált sérülékenységelemző

[35] 185/2015. (VII. 13.) kormányrendelet, 1. § 5. pont.
[36] 185/2015. (VII. 13.) kormányrendelet, 1. § 2. pont.
[37] 185/2015. (VII. 13.) kormányrendelet, 1. § 7. pont.
[38] 185/2015. (VII. 13.) kormányrendelet, 1. § 3. pont.
[39] 185/2015. (VII. 13.) kormányrendelet, 1. § 8. pont.
[40] 185/2015. (VII. 13.) kormányrendelet, 1. § 13. pont.

szoftverek használatával kezdődnek, majd technológiától és egyéb szempontoktól, valamint az automata vizsgálat eredményétől függően intuitív kézi elemzésre is szükség lehet.

A vezeték nélküli hálózat informatikai biztonsági vizsgálata alkalmával a vezeték nélküli hozzáférési és kapcsolódási pontok keresése, feltérképezése, a titkosítási eljárások elemzése, a titkosítási kulcsok visszafejthetőségének ellenőrzése célszoftverek és kézi vizsgálat útján történik.[41] Ezenkívül sor kerülhet az elérhető vezeték nélküli hálózatok sebezhetőségének vizsgálatára célszoftverek segítségével, hamis vezeték nélküli hozzáférési pont installálására és a kliensek forgalmának eltérítési kísérletére, a vezeték nélküli kapcsolódási házirend alkalmazásának tesztelésére, valamint a hálózati eszközök naplózási beállításainak vizsgálatára.

Jogosultsági szintek

A megrendelő által biztosított jogosultsági szintek alapján megkülönböztetünk regisztrált felhasználói jogosultság nélküli (black box), regisztrált felhasználói (korlátozott) jogosultsággal rendelkező (grey box), valamint adminisztrátori jogosultsággal rendelkező (white box) vizsgálatokat. Az egyes vizsgálatoknak más és más a célja, ezért szükséges ez a megkülönböztetés.

A regisztrált felhasználói jogosultság nélküli informatikai biztonsági vizsgálat egy olyan eljárás, amelynek során a vizsgálatot végző személy semmilyen előzetes információval nem rendelkezik az érintett szervezet informatikai rendszeréről, és nincs felhasználói jogosultsága a rendszerhez.[42]

A regisztrált felhasználói jogosultsággal rendelkező informatikai biztonsági vizsgálat során a vizsgálatot végző személy a számára külön létrehozott felhasználói jogosultsággal végzi a vizsgálatot.[43]

Az adminisztrátori jogosultsággal rendelkező informatikai biztonsági vizsgálat alkalmával a vizsgálatot végző személy rendszergazdai jogosultsággal rendelkezik, és az eljárás célja, hogy megfelelőségi listák alapján az érintett szervezet teljes informatikai rendszerének állapotát ellenőrizzék.[44]

3.1.6.2. A sérülékenységvizsgálati projekt kezdete

A sérülékenységvizsgálati projektek keletkezhetnek beérkező ügyfélmegrendeléssel vagy hatósági elrendeléssel. A GovCERT ügyfelei a korábban részletezett típusú vizsgálatokat kezdeményezhetik, valamint a hatóság végzésben is kötelezhet ügyfelet meghatározott vizsgálatok elvégeztetésére.

Egy bejövő megrendelés esetén meg kell állapítani, hogy a szervezet jogosult-e vizsgálatot kezdeményezni, valamint kapacitásfelmérést kell végezni annak érdekében, hogy a vizsgálatot mindkét fél számára kedvező véghatáridővel bonyolítsák le.

A megrendelő feladata a vizsgálati kezdeményezés okának és lényeges körülményeinek ismertetése, annak a megállapítása céljából, hogy a vizsgálandó rendszer a GovCERT kizárólagos sérülékenységvizsgálati hatáskörébe tartozik-e, illetve mi a vizsgálat kezdeményezésének indoka (új rendszer vagy szolgáltatás bevezetése, meglévő rendszer vagy szolgáltatás felülvizsgálata stb).

A vizsgálatokat a központ elosztott erőforrásból, projektszerűen valósítja meg; ennek célja az erőforrások minél hatékonyabb felhasználása és elosztása. A sérülékenységvizsgálati projektek általában több munkatárs csapatmunkáján alapulnak: a kollégák különböző vizsgálatok szakszerű és alapos végrehajtására szakosodnak annak érdekében, hogy a különböző vizsgálati típusokat és módszereket a legnagyobb szakértelemmel és naprakész tudással végezhessék.

Egy-egy vizsgálatban egy elemző központi koordinációs szerepet, úgynevezett projektgazdai pozíciót tölt be, akit a jogosultság- és kapacitásvizsgálatot követően a projekt kezdeti szakaszában

[41] 185/2015. (VII. 13.) kormányrendelet, 1. § 14. pont.
[42] 185/2015. (VII. 13.) kormányrendelet, 1. § 9. pont.
[43] 185/2015. (VII. 13.) kormányrendelet, 1. § 10. pont.
[44] 185/2015. (VII. 13.) kormányrendelet, 1. § 1. pont.

jelölnek ki. Nagyobb projektek esetén, a terhek megosztása érdekében kijelölhetnek egy helyettes projektgazdát is. A projektgazda felelős a vizsgálat sikeres lebonyolításáért a kezdetektől egészen a végső jelentés elkészüléséig, annak kiküldéséig, valamint az utókövetésig. A projektgazda felelős továbbá a felek közötti találkozók megszervezésért, az azokra való felkészülésért, oroszlánrészt vállal a dokumentációk elkészítésében, ő az elsődleges kapcsolati pont a vizsgálatot végző csapat és a megrendelő között. Ezenkívül összehangolja a csapat működését is, a szakterület vezetőjével közösen részt vállal a tervezésben.

A kapcsolattartás elsődleges formája a telefon és az e-mail, azonban több projekt esetén szükséges személyes egyeztetés is. Ezen részt vesz a megrendelő oldaláról felelős személy (vezető), az érintett szakterület vagy projekt képviselője és esetenként a fejlesztő is.

A vizsgálat különböző szakaszainak nyomon követése, auditálása miatt a GovCERT egy többfunkciós projektmenedzsment-rendszert használ. Az alkalmazás segítségével lehetőség nyílik a projekttel kapcsolatos adatok biztonságos tárolására, a feladatok hatékony elosztására, különböző státuszok használatára, a feladatok haladásának nyomon követésére, az elakadások detektálására, a vezetők gyors és hatékony tájékoztatására.

A kezdeti szakaszban kiküldenek az intézménynek egy általános tájékoztatót és egy adategyeztető lapot, amelyek segítik az ügyfelet a zökkenőmentes kapcsolatfelvételben és adategyeztetésben, a vizsgálati lehetőségek megismerésében, valamint a projekt céljának megértésében, a projektgazdával történő hatékony együttműködésben.

Az általános tájékoztatóban leírják a módszertani elemeket, az irányultságokat és a jogosultságokat, ez tartalmazza továbbá a különböző módszerek részletes leírását, valamint a sérülékenységelemzési módszertant és a javaslatok kidolgozásának metodikáját. Az adategyeztető lap információkat kér a megrendelőtől a vizsgálat indokáról, céljáról, a vizsgált rendszerről, a különböző dokumentumokról (osztályba sorolás, rendszerdokumentumok stb.), valamint a végrehajtással kapcsolatos adatokról (kapcsolattartók, technikai feltételek stb.).

A sérülékenységvizsgálat végrehajtásának személyi, technikai, időbeli és egyéb feltételei vannak.

Személyi feltétel azon kapcsolattartó személyek kijelölése, akik a vizsgálattal érintett felek (a vizsgáló, a vizsgált rendszer tulajdonosa, a vizsgált rendszer üzemeltetője stb.) között a közvetlen kapcsolattartásért felelősek. Technikai feltételként szükséges a hozzáférési jogosultságok biztosítása, valamint a fizikai és logikai összeköttetések létrehozása. Időbeli kötöttségként jelentkezik az egyes sérülékenységvizsgálati feladatokhoz rendelhető, javasolt kezdési és befejezési időpontok meghatározása.

Ezeken kívül jelentkezhetnek egyéb befolyásoló, illetve korlátozó tényezők, amelyek a hatással lehetnek a sérülékenységvizsgálat lefolytatására (például projektütemezés, a rendszer használatában vagy környezetében várható változások, a vizsgálatból kizárt kritikus szolgáltatások vagy kritikus időszakok stb.).

A vizsgálandó rendszerekről, illetve a vizsgálandó funkcionalitásról rendelkezésre álló releváns adatokat tartalmazó alábbi dokumentációkra elektronikus formában lehet szüksége az elemzést végző csapatnak:

- a törvény szerinti biztonsági osztályba sorolással kapcsolatos dokumentumok (amennyiben ezeket korábban a GovCERT vagy NEIH részére átadták, akkor ezek hivatkozási számai),
- a korábbi, nem hatósági ellenőrzések (auditok) és sérülékenységvizsgálatok dokumentációi,
- rendszerdokumentációk, ezen belül a fizikai és logikai hálózati topológia, a rendszerelemek, a külső kapcsolatok és külső elérhetőségek jegyzéke,
- a védelmi infrastruktúrával kapcsolatos dokumentációk, a biztonsági rendszerelemeket és konfigurációjukat, ezen belül is a határvédelmet, naplózást, IDM-et, IDS/IPS-t, a jogosultságmenedzsmenti információkat tartalmazó üzemeltetési és telepítési kézikönyv,
- az alkalmazásdokumentációk (funkciók, interfészek stb.), a kritikus szolgáltatások megjelölése,
- az átadandó dokumentumok jegyzéke, amely tartalmazza a dokumentum megnevezését (fájlnév), leírását, terjedelmét, kiadási dátumát és a tartalom érvényességét (naprakészségét),

- azon – az Ibtv. és végrehajtási rendeletein túlmutató – jogszabályi előírások vagy egyéb szabályzatok jegyzéke, amelyeknek funkcionális vagy biztonsági szempontból meg kell feleltetni a vizsgálandó elektronikus információs rendszerüket.

A projektalapító dokumentum

Az adategyeztető lap kitöltésének ellenőrzését, valamint a hiánypótlásokat és javításokat követően kerülhet sor a vizsgálat alapjául szolgáló projektalapító dokumentum elkészítésének megkezdésére. A dokumentációban a GovCERT rögzíti a vizsgálati feladatokat, a célokat, a technikai és személyi feltételeket, a módszertant, az egyeztetések idejét, a sérülékenységvizsgálat várható befejezésének dátumát, az eredménytermékeket, a kritikus tényezőket, a siker mérésének módszertanát.[45] A dokumentumot általában a projektgazda készíti el és egyezeti a megrendelővel.

Ha a vizsgálatot a NEIH rendeli el, akkor a sérülékenységvizsgálati dokumentációban a határozatban rögzített vizsgálati feladatokat kell feltüntetni. A sérülékenységvizsgálat egyedi kezdeményezése esetén a vizsgálati feladatokra a kezdeményező javaslatot tehet, amelyről a GovCERT vezetője dönt.[46]

A projektalapító dokumentumot a GovCERT – minden esetben belső ellenőrzést és jóváhagyást követően – egyezetés céljából megküldi az érintett szervezet részére, általában elektronikus (PDF) formában. Az érintett szervezet a dokumentáció tartalmára a kézhezvételtől számított nyolc napon belül észrevételt tehet. Az észrevétel nem érintheti a hatóság által elrendelt vizsgálatokat. Az észrevételekről a GovCERT jogosult dönteni.[47]

Egyetértés esetén a felek, tehát a megrendelő megfelelő jogosultsággal rendelkező munkatársai és a Nemzeti Kibervédelmi Intézet vezetője elfogadják és aláírásukkal hitelesítik a dokumentumot.

A projektalapító dokumentum elkészültét követően történik a vizsgálat tervezése. A tervezés célja a megfelelő erőforrás-menedzsment, az ütemezéssel a hatékonyság növelése és a párhuzamosságok elkerülése. Sor kerül a lépések megtervezésére, a terv dokumentálására, valamint a vizsgálathoz szükséges hozzáférések beszerzésére. Amennyiben a vizsgálat lefolytatása megköveteli, indokolt rendszerbeavatkozási kérelmet is elküldenek az intézménynek, valamint szükség esetén további egyeztetés is kezdeményezhető az érintett szervezettel.

3.1.6.3. A sérülékenységvizsgálat lefolyása

A Kormányzati Eseménykezelő Központ az általánosan bevett eljárások, a különböző nemzetközi módszertanok, a „legjobb szakmai gyakorlatok” (*best practices*) és trendek szerint, a projektalapító dokumentumban és a kormányrendeletben lefektetett keretekben és módon végzi a vizsgálatait.

A GovCERT a sérülékenységvizsgálat során kellő gondossággal eljárva törekszik a vizsgált elektronikus információs rendszer által nyújtott szolgáltatások szükségesnél nem nagyobb mértékű korlátozására, a vizsgálatnak a szolgáltatás szempontjából nem kritikus időszakban történő elvégzésére. A GovCERT feladata a korlátozás várható mértékéről és időtartalmáról az érintett szervezetet előzetesen tájékoztatni.[48]

Hatósági határozat alapján elrendelt vizsgálat esetén az érintett szervezet köteles a sérülékenységvizsgálat lefolytatásához szükséges adatokat, dokumentumokat, eszközöket és egyéb információkat a Kormányzati Eseménykezelő Központ rendelkezésére bocsátani, ezenfelül tűrni a sérülékenységvizsgálatból fakadó, a vizsgált elektronikus információs rendszeren bekövetkezett szolgáltatáscsökkenést.[49]

[45] 185/2015. (VII. 13.) kormányrendelet, 17. § (1) bekezdés.
[46] 185/2015. (VII. 13.) kormányrendelet, 17. § (2) bekezdés.
[47] 185/2015. (VII. 13.) kormányrendelet, 17. § (3) bekezdés.
[48] 185/2015. (VII. 13.) kormányrendelet, 16–18. § (1) bekezdés.
[49] 185/2015. (VII. 13.) kormányrendelet, 16–18. § (2) bekezdés.

Egyedi kezdeményezés esetén az érintett szervezet kizárhatja azon vizsgálatokat, amelyek jelentős szolgáltatáscsökkenést eredményeznek a rendszerben.[50] Jellemzően ilyen lehet a szolgáltatásmegtagadásos támadások különböző módszereinek tesztelése.

A vizsgálatok közben folyamatosan dokumentálás történik, amely a későbbi jelentés alapjául szolgál. A dokumentálásban szöveges leírásokat, valamint a találatok alátámasztására szolgáló adatokat, speciális fájlokat, képernyőképeket mentenek el. Amennyiben ezt az érintett szervezet igényli, akkor az egyes sérülékenységek felderítésekor azonnali értesítést kaphat a kockázatok mérséklése érdekében.

A határidők

A vizsgálat határideje a hatóság határozatának keltétől, illetve az előzetesen egyeztetett kezdési időponttól számítva külső informatikai biztonsági vizsgálat esetén harminc nap, webes vizsgálat esetén hetvenöt nap, belső informatikai biztonsági vizsgálat esetén kilencven nap, a vezeték nélküli hálózat informatikai biztonsági vizsgálat esetén harminc nap.[51] A GovCERT a sérülékenységvizsgálatra irányadó határidőt annak letelte előtt egy alkalommal, legfeljebb harminc nappal meghosszabbíthatja, és erről az érintett szervezetet, valamint hatóságot értesíti.[52]

Az átlagostól eltérő elektronikus információs rendszerek esetén az elemzés összetettsége miatt speciális határidős szabályokat lehet alkalmazni.

Az érintett szervezet elektronikus információs rendszere az átlagostól jelentősen eltér, ha az elektronikus információs rendszer a külső internetes tartományban több mint 20, IP-címen elérhető eszközzel, több mint 10 webes szolgáltatással, a belső hálózatban több mint 50 szerverrel, több mint 500 munkaállomással, több mint 5 vezeték nélküli hálózattal vagy több mint 500 fős felhasználói létszámmal rendelkezik. Ha az érintett szervezet több mint három telephelyen rendelkezik a vizsgálattal érintett elektronikus információs rendszerrel, szintén átlagostól eltérőnek minősül.[53]

Ha az érintett szervezet elektronikus információs rendszere, rendszereleme az átlagostól jelentősen eltér, és emiatt egyedi vizsgálati eljárás szükséges, a sérülékenységvizsgálati határidő további harminc nappal meghosszabbítható.[54]

A vizsgálatot nehezítő, akadályozó körülmények kezelése

Ha a projektalapító dokumentumban foglalt feltételrendszer a vizsgálat elindulásakor azonnal vagy a projekt közben nem áll fenn, a megrendelő tájékoztatása haladéktalanul megtörténik, valamint a Gov CERT tájékoztatást kér a feltétel fennállásáról. Ezt minden esetben ellenőrzik, és a projektgazda értesíti a megrendelőt a sikerességről.

Előállhatnak olyan esetek, amikor a projekt haladásának érdekében köztes egyeztetésre van szükség, amely általában személyes találkozót igényel. A megbeszélésen a felelős vezetőkön kívül általában az illetékes szakemberek, a fejlesztők és a vizsgálatot végzők vesznek részt.

Amennyiben az elem valamely okból nem állítható vissza, akkor meg kell vizsgálni, hogy a vizsgálat további folytatásához szükséges-e módosítani a projektalapító dokumentumot. Amennyiben a vizsgálat enélkül nem folytatható, a módosítás az egyeztetésre vonatkozó szabályokat betartva történik.

[50] 185/2015. (VII. 13.) kormányrendelet, 16–18. § (3) bekezdés.
[51] 185/2015. (VII. 13.) kormányrendelet, 16. § (3) bekezdés.
[52] 185/2015. (VII. 13.) kormányrendelet, 16. § (4) bekezdés.
[53] 185/2015. (VII. 13.) kormányrendelet, 19. § (1) bekezdés.
[54] 185/2015. (VII. 13.) kormányrendelet, 19. § (1) bekezdés.

Kritikus sérülékenység kezelése

Amennyiben a GovCERT kritikus besorolású sérülékenységre bukkan a vizsgálat során, arról minden esetben azonnali hatállyal tájékoztatja a megrendelő intézmény kapcsolattartó személyét.

Kritikusnak tekinthető az a sérülékenység, amely a bizalmasságot, sértetlenséget vagy rendelkezésre állást nagymértékben sérti, illetőleg a sérülékenység távolról, könnyedén vagy hitelesítés nélkül kihasználható.

A sérülékenységről szóló jelentést belső ellenőrzést és jóváhagyást követően, amennyiben erre lehetőség van, szóban és írásban közlik a megrendelő szerv felelős vezetőjével.

Amennyiben a sérülékenység biztonsági esemény is egyben, a projektgazda gondoskodik az incidens bejelentéséről. Ebben az esetben a bejelentés észlelésnek minősül, és az eset kezelése a korábban ismertetett eljárás szerint történik.

3.1.6.4. A sérülékenységvizsgálat lezárása

A sérülékenységvizsgálat lezárásakor a központ minden esetben állásfoglalást készít. A szakértők részletes jelentése alapján sor kerül a kockázatok értékelésére, valamint a feltárt sérülékenységek kezeléséhez szükséges javaslatokkal segítik a megrendelők későbbi munkáját.

Az állásfoglalás elkészítését belső szakmai ellenőrzés és jóváhagyás követi. A GovCERT az elkészült dokumentumot nyolc napon belül megküldi az érintett szervezet és – hatósági kezdeményezés esetén – a NEIH részére.[55] Az állásfoglalás tartalmazza a vizsgálati eredmények leírását, valamint a rövid, közép- és hosszú távú intézkedésekre vonatkozó javaslatokat.[56]

A GovCERT állásfoglalása az esetek többségében tartalmazza a tapasztalatokat összegző vezetői összefoglalót, melyben megjelennek a javasolt cselekvési folyamatok és egy kockázati összesítő is. A kockázatokat értékelő fejezet meghatározza a kockázati szinteket, magukat a – kritikus, magas, közepes és alacsony kategóriákba sorolt – kockázatokat. A vizsgálatok műszaki leírásában a vizsgálati módszereket, a használt technológiákat ismertetik.

Az állásfoglalást követően, az intézmény kérése esetén a projekt gazdája prezentáció keretében mutatja be a sérülékenységvizsgálat eredményét megjelenítő dokumentumokat, és az esetlegesen felmerülő kérdések megválaszolására is sor kerülhet.

3.1.6.4. A sérülékenységvizsgálat egyéb szabályai

A polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereinek sérülékenységvizsgálatát az IntCERT,[57] a honvédelmi célú elektronikus információs rendszerek vizsgálatát a MilCERT végzi.[58]

A kormányrendelet lehetőséget biztosít külső sérülékenységvizsgálattal foglalkozó gazdasági társaság bevonására is. Külső társaságok abban az esetben végezhetnek vizsgálatot, ha a gazdasági társaság nevében és alkalmazásában eljárva a vizsgálatban részt vevő személy a törvényben meghatározott feltételeken túl rendelkezik a vizsgálat lefolytatásához szükséges ismeretek meglétét igazoló végzettséggel, ezen a szakterületen legalább 2 év szakmai tapasztalattal, valamint a gazdasági társaságot bejegyezték a sérülékenységvizsgálat lefolytatására jogosult gazdasági társaságok nyilvántartásába.[59]

[55] 185/2015. (VII. 13.) kormányrendelet, 20. § (1) bekezdés.
[56] 185/2015. (VII. 13.) kormányrendelet, 20. § (2) bekezdés.
[57] 185/2015. (VII. 13.) kormányrendelet, 14. § (2) bekezdés.
[58] 185/2015. (VII. 13.) kormányrendelet, 14. § (3) bekezdés.
[59] 185/2015. (VII. 13.) kormányrendelet, 14. § (4) bekezdés.

A sérülékenységvizsgálat lefolytatására jogosult gazdasági társaságokról az Alkotmányvédelmi Hivatal olyan nyilvántartást vezet, mely személyes adatot nem tartalmaz, azonban szerepelnek benne az érintett gazdasági társaság adatai, a vizsgálatban részt vevő személyek száma és a vizsgálatok lefolytatásához szükséges ismereteket igazoló végzettség megnevezése és megszerzési ideje.[60]

A nyilvántartásba való felvételt a gazdasági társaság kezdeményezi az Alkotmányvédelmi Hivatalnál, a feltételek meglétét igazoló okiratok benyújtásával, a feltételek szakmai megfelelőségében a GovCERT nyilatkozata az irányadó.[61]

3.1.7. A GovCERT támogató és koordinációs feladatai

A kormányrendeletben foglaltak alapján a központ nem kötelező érvényű állásfoglalásokat, ajánlásokat adhat ki, a biztonsági események kezelésére irányuló tájékoztatót tarthat, részt vehet az információbiztonság tudatosításáért felelős intézmények tudatosítási programjában, szakértői-oktatói tevékenységet végezhet. Ezeken kívül a GovCERT kormányzati információtechnológiai, hálózatbiztonsági és biztonságiesemény-kezelési együttműködési fórumot működtethet, részt vesz az infokommunikációs biztonságra vonatkozó stratégiák és szabályozások előkészítésében.[62]

3.1.7.1. Tudatosító tevékenység

A központ a tudatosító tevékenysége keretében különböző eseményeken vesz részt, tájékoztató és tudatosító anyagokat készít és terjeszt, tudatosítási kampányokat szervez.

A különböző eseményeken való részvétellel, valamint a sajtómegkeresések kezelésekor a GovCERT elsődleges célja az információbiztonsági tudatosító tevékenység, a szervezetek és az egyének figyelmének ráirányítása a probléma fontosságára.

Az utóbbi években a GovCERT dolgozói rendszeres szereplői a különböző iparági konferenciáknak. Hol általános témáról, kiberstrarégiáról, az NKI szerepéről, hol technikai témákról igyekeznek minél színvonalasabb előadásokat tartani. 2016-ban hagyományteremtő szándékkal elindult az intézet önálló konferenciája cybersecurity2016.hu néven.

A sajtómegkeresések száma folyamatosan növekszik, 2016-ban több mint 50 ilyen jellegű felkérés érkezett. Az intézet törekszik a lehető legpontosabb és leggyorsabb tájékoztatásra, ennek érdekében sajtóreferens segíti a kollégák munkáját.

Az intézet munkatársai több tanfolyam, oktatás keretében is tartanak előadást oktatási intézményeknél. Az utóbbi időben a Nemzeti Közszolgálati Egyetem és az Óbudai Egyetem katedráin hallhattak a hallgatók az NKI tevékenységeiről részletesebb előadásokat.

Meghívás esetén ügyfeleknél, partnereknél is tartanak előadásokat az általános előadástól egészen a technikai jellegű speciális témákig. Az egyik leggyakrabban előadott téma a felhasználói tudatosság erősítését célozza, amit konkrét incidensek bemutatásával lehet a leghatékonyabban elérni. Ezeken kívül tájékoztató és tudatosító anyagok, sajtószemle is készül, melyeket a weboldalon vagy fizikai formában nyomtatva is közzétesznek.

Az intézet a tudatosítási kampányok szervezéséből is kiveszi a részét. Az egyik legismertebb ilyen az ECSM (European Cyber Security Month, az Európai Kiberbiztonsági Hónap), amelyet minden év októberében rendeznek meg. A kampányt az ENISA szervezi, Magyarországon a GovCERT koordinálja a lebonyolítást. 2016-ban több mint 10 kapcsolódó rendezvényt tartottak, tájékoztatók és egyéb anyagok közzétételével.

---

[60] 185/2015. (VII. 13.) kormányrendelet, 14. § (5) bekezdés.
[61] 185/2015. (VII. 13.) kormányrendelet, 14. § (7) bekezdés.
[62] 185/2015. (VII. 13.) kormányrendelet, 5. § (4) bekezdés.

3.1.7.2. Technikai tanácsadás

Incidenshez kötötten, általánosságban vagy új rendszerhez kapcsolódóan a központ technikai tanácsadói tevékenységet is végez, elsősorban ügyfelei részére, rendkívüli esetekben azonban partnereinek és magánszemélyeknek is.

A tanácsadás módja lehet általános tájékoztatás vagy technikai jellegű, konkrét tanácsok kidolgozása is. Az utóbbi eset mélyebb információkat igényel a tanácsadásban érintett eseményről, rendszerről.

3.1.7.3. Kibervédelmi gyakorlatok

A Nemzeti Kibervédelmi Intézet, hogy munkatársainak tudását naprakészen tartsa, valamint az új ismeretek és gyakorlatok megszerzése miatt elkötelezett a kibervédelmi gyakorlatok iránt.

A gyakorlatoknak több típusa is ismert. A *CommCheck gyakorlat* célja a kommunikációs lánc működésének, gyorsaságának ellenőrzése. Az *incidenskezelési (procedurális) gyakorlat* célja az eljárások tesztelése, egy *komplex gyakorlat* pedig technikai képességeket, konkrét incidenskivizsgálást is igényel. Ezenkívül egyéb, célzott képességek tesztelésére irányuló gyakorlat is elképzelhető.

A résztvevők köre alapján megkülönböztetünk *szervezeten belüli, ágazati, nemzeti, regionális vagy nemzetközi gyakorlatokat.*

A gyakorlatokban való részvétel több mélység szerint tagozódik. Az együttműködési vagy megfigyelési szinten külső szemlélőként, tapasztalatszerzési célból vonnak be egy-egy szervezetet. A részvétel szinte aktív közreműködést feltételez, jogokkal és kötelességekkel jár. A koordinációs szerepre akkor van szükség, ha például egy nagy nemzetközi gyakorlat regionális vagy nemzeti részét kell lebonyolítani. A legösszetettebb feladat pedig a teljesen saját gyakorlat szervezése.

3.1.7.4. Kiberbiztonsági koordináció és nemzetközi szerepvállalás

A Nemzeti Kibervédelmi Intézet részt vesz Magyarország kiberstratégiájának megalkotásában, részt vállal annak megvalósításában. Felkérésre a kompetenciakörébe tartozó jogszabályok véleményezésében is közreműködik. Az elkövetkező időkben nagy feladatként jelentkezik a központ életében az Európai Unió hálózatbiztonsági irányelvének (*NIS directive*) implementációja a magyar jogba. Ennek és egyéb koordinációs tevékenységének keretében folyamatos kapcsolatot tart ügyfeleivel, az eseménykezelőkkel, valamint partnereivel belföldön és külföldön egyaránt.

A nemzeti CERT szerepkörnek megfelelően az intézet képviseli Magyarországot számos nemzetközi fórumon, az Európai Unió szakbizottságaiban, az ENISA-nál, a CSIRT-ek nemzetközi hálózatában és egyéb együttműködésekben.

A Nemzeti Kibervédelmi Intézet aktív szakmai támogatást biztosít a Nemzeti Kiberbiztonsági Koordinációs Tanács részére, valamint támogatja a kormányzati tevékenység összehangolásáért felelős miniszter által delegált kiberkoordinátor munkáját is.

3.1.8. Hatósági tevékenység

A Nemzeti Elektronikus Információbiztonság Hatóság jogszabályi működési kereteit az információbiztonságról szóló törvény, valamint annak végrehajtási rendelete és számos egyéb jogszabály adja. A hatóság ügyfélkörét a törvény jelöli ki, amely nagy vonalakban megegyezik a Kormányzati Eseménykezelő Központ ügyfélkörével.

A hatóság az egyik legfontosabb feladataként elbírálja a törvény hatálya alá tartozó elektronikus információs rendszerek biztonsági osztályba sorolását, valamint ellenőrzi az elektronikus információs

rendszerek biztonsági osztályba és a szervezetek biztonsági szintbe sorolására vonatkozó jogszabályi követelmények teljesülését.

A rendelkezésre álló információk alapján kockázatelemzést végez, és az éves ellenőrzési terv alapján az érintett ügyfeleknél ellenőrzi az információbiztonsági követelményeknek való megfelelést. Ezen túlmenően a hatóság elrendeli az ellenőrzés során feltárt vagy más módon tudomására jutott biztonsági rések elhárítását, ellenőrzi a helyreállító intézkedés eredményességét.

A hatóság a tevékenységéről éves jelentést készít a kormány részére az elektronikus információs rendszerek biztonságával, a létfontosságú információs rendszerelemek védelmével és a kibervédelem helyzetével kapcsolatban.

A NEIH részére – feladata ellátásához – széles együttműködői kört írnak elő a jogszabályok. Az Elektronikus Ügyintézési Felügyelettel a szabályozott elektronikus ügyintézési szolgáltatókra vonatkozó biztonsági követelmények biztosításában működik együtt a hatóság, és a Kormányzati Eseménykezelő Központtal, valamint a Nemzeti Kiberbiztonsági Koordinációs Tanáccsal is van kapcsolódási pontja.

Ügyfelei számára engedélyezi és felügyeli az elektronikus információs rendszerek EGT-államban való üzemeltetését, valamint a központi és az európai uniós forrásból megvalósuló fejlesztési projektek tervezési szakaszában ellenőrzi az információbiztonsági követelmények megtartását.

A hatóság célja nem a büntetés, hanem az ügyfelek hatékony támogatása. Célja továbbá, hogy hangsúlyozza az elektronikus információbiztonság egységes kezelésének szükségességét az állami és önkormányzati szervek körében.

A hatóság a partnerekkel való kapcsolattartás során nagy hangsúlyt fektet a kölcsönös együttműködés kialakítására, illetve arra, hogy szolgáltató hatóságként segítséget tudjon nyújtani partnereinek. Fontos, hogy kialakuljon a szervezetek bizalma a hatóság felé, ezt adataik bizalmas kezelésével és a támogatói attitűd felmutatásával segítik elő.

3.1.8.1. A hatósággal kapcsolatos alapfogalmak

A biztonsági osztály az elektronikus információs rendszer védelmének elvárt erőssége,[63] melyhez 1-től 5-ig számozott fokozatot kell rendelni. A számozás emelkedésével párhuzamosan szigorodnak a rendszerre vonatkozó védelmi előírások is.[64] A biztonsági osztályba sorolás a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározásának folyamata, melyet saját rendszerére vonatkozóan az ügyfél végez el.[65]

A biztonsági szint a szervezet felkészültsége a törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére.[66] A kockázatokkal arányos, költséghatékony védelem kialakítása érdekében magát a szervezetet kell az elektronikus információs rendszerek védelmére való felkészültsége alapján biztonsági szintbe sorolni.[67] A biztonsági szintbe sorolás a szervezet felkészültségének meghatározása a jogszabályokban meghatározott biztonsági feladatok kezelésére.[68]

3.1.8.2. A hatóság által kezelt adatok

A NEIH-nek tevékenysége maradéktalan és magas szintű ellátásához adatok kezelésére van szüksége. Ennek keretében kezeli az ügyfeleinek azonosításhoz szükséges szervezeti adatokat, az elektronikus

[63] 2013. évi L. törvény, 1. § 11. pont.
[64] 2013. évi L. törvény, 7. § (2). bekezdés.
[65] 2013. évi L. törvény, 1. § 12. pont.
[66] 2013. évi L. törvény, 1. § 13. pont.
[67] 2013. évi L. törvény, 9. § (1) bekezdés.
[68] 2013. évi L. törvény, 1. § 14. pont.

információs rendszer biztonságáért felelős személy azonosító adatait, telefon- és telefaxszámát, e-mail-címét, végzettségét és a szakképzettséget igazoló okiratok másolatát.

Ezenkívül tárolja a szervezetek informatikai biztonsági szabályzatát, az ügyfelek elektronikus információs rendszereinek biztonsági osztályát és a 41/2015 (VII. 15.) BM rendeletben meghatározott technikai adatait, az ügyfelek biztonsági szintjét.

Tárolni és kezelni szükséges még az ügyfélre vonatkozó információbiztonsági követelményekben felmerülő hiányosságok megszüntetésére vonatkozó cselekvési tervet is.

Az adatkezelési tevékenység zökkenőmentes tárolása érdekében a NEIH személyre szabott, a feladatának ellátását hatékonyabbá és gyorsabbá tevő adatbázist használ, amelyet bizalmasan kezel.

3.1.8.3. Ügytípusok

A hatóság megkülönböztet *csak hivatalból, csak kérelemre,* illetve kérelemre és hivatalból is induló eljárásokat. A kérelemre és hivatalból is induló eljárások a szervezet regisztrációja, illetve az adatbejelentés.

A szervezet a hatóság elektronikus adatbejelentésre szolgáló felületén keresztül be tudja jelenteni az elektronikus információs rendszer biztonságáért felelős személy jogszabályban előírt adatait. Az elektronikus információs rendszer biztonságáért felelős személy a szervezet nevében a hatóság elektronikus adatbejelentő felületén keresztül tudja regisztrálni a szervezetet. A regisztrációt követően a szervezet vezetője a hatóság elektronikus adatbejelentő rendszere által automatikusan előállított regisztrációs űrlap hitelesített példányát biztonságos elektronikus kézbesítési szolgáltatással vagy postai úton küldi meg a hatóság számára.[69]

Hatósági adatbejelentésnek minősül, amennyiben az ügyfél megküldi a NEIH részére a szervezet elektronikus információs rendszereinek megnevezését, az elektronikus információs rendszerek biztonsági osztályának és a szervezet biztonsági szintjének besorolását, az elektronikus információs rendszerek külön jogszabályban meghatározott technikai adatait és a szervezet informatikai biztonsági szabályzatát[70] Adatbejelentést csak sikeres regisztrációt követően van lehetősége tenni a szervezetnek.

Ha a regisztrációt vagy az adatbejelentést az ügyfél szervezet kezdeményezte, akkor az eljárás kérelemre induló hatósági eljárásnak minősül. Ha mindezt az ügyfél szervezet a hatóság felszólítására végezte el, akkor arra a hivatalból induló eljárás szabályait kell alkalmazni.

Kizárólag kérelemre indul az állásfoglalás kérése, az alacsonyabb biztonsági osztályba vagy szintbe sorolás és a külföldi adatkérés engedélyese.

A hatóság ügyfele a NEIH hatáskörébe tartozó kérdésekben állásfoglalási kérelmet nyújthat be. A kérelmet írásban kell benyújtani. Az állásfoglalás hatálya kizárólag a kérelmező ügyfélre terjed ki. Az állásfoglalást a hatóság az ügyféllel lefolytatott további eljárásokban kötelező érvénnyel veszi figyelembe, amíg új körülmény nem merül fel, illetve jogszabály eltérően nem rendelkezik.

Amennyiben az ügyfél az elektronikus információs rendszerére a jogszabályi alapértelmezettnél alacsonyabb biztonsági osztályt kíván megállapítani, írásbeli kérelmet kell benyújtania a hatóságnak. Alacsonyabb biztonsági szint meghatározását a létfontosságú információs rendszerelemmel rendelkező szervezet kezdeményezheti.[71]

A törvény lehetőséget ad arra, hogy egyes ügyfelek bizonyos elektronikus információs rendszereiket Magyarország területén kívül üzemeltetessék, illetve azokban külföldön végezzenek adatkezelést. Az ügyfél – kivéve a Magyar Honvédséget – ebben a tárgyban az adatkezelés kezdetét legalább 90 nappal megelőzően írásbeli kérelmet nyújthat be a hatósághoz.[72]

---

[69] 42/2015. (VII. 15.) BM rendelet, 2. § (1)–(3) bekezdés.
[70] 2013. évi L. törvény, 15. § (1) bekezdés b) és d) pontjai.
[71] 2013. évi L. törvény, 9. § (6) bekezdés.
[72] 2013. évi L. törvény, 3. § (2)–(3) bekezdés.

Csak hivatalból induló eljárás a működő elektronikus információbiztonsági rendszer ellenőrzése és az informatikai projekt biztonsági ellenőrzése.

A hatóság jogosult az ügyfél szervezet elektronikus információs rendszereire irányadó adminisztratív, fizikai és logikai biztonsági követelményeinek megtartását ellenőrizni.[73] Az ellenőrzés hivatalból, éves ellenőrzési terv alapján vagy soron kívül indul meg. A hatóság a döntését logikai védelmi intézkedések vizsgálatakor 120 nap alatt, egyéb esetben 30 nap alatt hozza meg, amelyben kötelezheti a szervezetet a hiányosságok meghatározott feltételek szerinti pótlására. Az éves ellenőrzési terv elkészítéséhez a hatóság a Kormányzati Eseménykezelő Központ incidenskezelése és sérülékenységvizsgálatai során szerzett tapasztalatait használja fel.

A Nemzeti Elektronikus Információbiztonsági Hatóság ellenőrzi az Európai Uniós forrásból a Közigazgatás- és Közszolgáltatás-fejlesztés Operatív Program (KÖFOP) keretében megvalósuló fejlesztésekre vonatkozó elektronikus információbiztonsági követelmények megvalósulását. Ennek keretében a pályázók előre meghatározott eljárásrend szerint működnek együtt a hatósággal.

3.1.8.4. A hatóság további jogkörei és feladatai

A Nemzeti Elektronikus Információbiztonság Hatóságot számos javaslattételi és véleményezési jog illeti meg: javaslatot tehet létfontosságú információs rendszerelemek kijelölésére, információbiztonsági, létfontosságú információs infrastruktúravédelmi, kibervédelmi gyakorlatokat szervezhet, valamint felkérésre képviselheti Magyarországot a nemzetközi információbiztonsági, létfontosságú információs infrastruktúravédelmi, kibervédelmi gyakorlatokon.

A NEIH véleményezheti a Kormányzati Eseménykezelő Központnak a biztonsági eseményekre való reagálás ágazatközi szabályairól és felelősségi köreiről szóló tervezetét, nem költségvetési szervekre indokolt esetben eljárási bírságot szabhat ki, költségvetési szervekhez információbiztonsági felügyelő kirendelését javasolhatja.

Az ügyfelek biztonságtudatosságának fejlesztésére érdekében a hatóság oktatási anyagokat dolgozhat ki, és felvilágosító kampányokat is szervezhet.

3.1.8.5. A GovCERT és a hatóság elhatárolása

Fontos elválasztani egymástól a Kormányzati Eseménykezelő Központ, valamint a Nemzeti Elektronikus Információbiztonság Hatóság tevékenységét. Ez egyszerűen úgy foglalható össze, hogy míg a hatóság a jogszabályi megfelelést vizsgálja, a GovCERT incidenskezelést végez.

A NEIH az intézmények jogszabályi megfelelőségi vizsgálatán túl támogatást nyújt és ellenőrzési jogkört gyakorol, míg a GovCERT technikai szinten nyújt támogatást, valamint technikai jellegű ellenőrzési tevékenységet végez.

A hatóság a tervezőasztaltól az elektronikus információbiztonsági rendszer életciklusának végéig folyamatosan, míg a központ incidens esetén vagy igény szerint végzi munkáját.

A NEIH megfelelőségi vizsgálatokkal, állásfoglalások és ajánlások kiadásával, valamint IT-biztonsági kontroll gyakorlásával, míg a GovCERT incidenskoordinációval, folyamatos tájékoztatással és sérülékenységvizsgálattal éri el célját.

[73] 2013. évi L. törvény, (1) bekezdés a)–c) pont.

3.1.9. Biztonságirányítás

Míg az NKI egyes szakterületei kívülről támogatják az állami és önkormányzati szerveket abban, hogy saját rendszereik védelmét ellássák, és ennek keretében kialakítsák saját, úgynevezett információbiztonsági irányítási rendszerüket, addig a biztonságirányítási szakterület ezt a feladatot tevőlegesen is végzi, részint az NKI biztonsági felügyeletére bízott, kiemelt kormányzati rendszerek esetében, részint pedig szakmai támogatást nyújtva a hatósági szakterület részére.

A biztonságirányítási szakterület kizárólagosan látja el a FAIR-ral és az EMIR-rel kapcsolatos informatikai biztonsági feladatokat, a kapcsolódó informatikai biztonsági fejlesztési feladatokat azonban közvetetten végzi. Az IMIR 2014–2020 informatikai biztonsági feladatait és az informatikai biztonsági fejlesztési feladatokat ez a szakterület kizárólagosan, egy közvetítő társaság útján látja el.[74]

A biztonságirányítási szakterület részt vesz a rendszerek biztonságos üzemeltetésében, valamint aktívan közreműködik a jogosultságkezelés biztonságával, az információbiztonsági és adatbiztonsági feladatok ellátásával kapcsolatban felmerülő feladatok ellátásában. A szakterületen belül egy úgynevezett Security Operation Centre (SOC) működik. A bizalmasságot, sértetlenséget és rendelkezésre állást akadályozó eseményekkel összefüggő incidenskezelési feladatokat, a megelőző tevékenységet speciális eszközök segítségével végzik, valamint a rendszereket ért eseményeket bejelentik a Kormányzati Eseménykezelő Központnak.

A szakterület folyamatos biztonsági jelentést készít az általa felügyelt rendszerek üzemeltetőjének, a Miniszterelnökségnek.

3.1.9.1. A védett rendszerek

A szakterület három pályázati rendszerrel kapcsolatban látja el tevékenységét.

Az *Egységes Monitoring és Információs Rendszer (EMIR)* az Európai Regionális Fejlesztési Alapból, az Európai Szociális Alapból, a Kohéziós Alapból, a PHARE-ból, az Átmeneti Támogatásból, a Schengen Alapból, az Európai Gazdasági Térség és Norvég Finanszírozási Mechanizmusból, valamint az ezekhez társuló hazai forrásokból megvalósuló programokkal és projektekkel kapcsolatos végrehajtási és kifizetési menedzsment-, monitoring-, valamint ellenőrzési, szabálytalanságkezelési és számviteli feladatokat támogató információtechnológiai rendszer.[75]

A *Fejlesztéspolitikai Adatbázis és Információs Rendszer (FAIR)* az európai uniós fejlesztési források felhasználására vonatkozó eljárások során keletkező adatok egységes nyilvántartási rendszere, mely három alrendszerből áll: az Európai Uniós Programok Rendszeréből, a Központi Rendszerből és a Nemzeti Pályázatkezelő Rendszerből.[76]

Az *IMIR 2014–2020* a 2014-től 2020-ig terjedő programozási időszakban az Európai Regionális Fejlesztési Alap, az Előcsatlakozási Támogatási Eszköz, valamint az Európai Szomszédsági Támogatási Eszköz nevű pénzügyi alapok területi együttműködéshez kapcsolódó egyes programjainak támogatásával megvalósuló programok és az azok keretében megvalósuló projektek adatainak gyűjtésére, rendszerezésére szolgáló informatikai rendszer.[77]

[74] 60/2014. (III. 6.) kormányrendelet, 25/A. § (2)–(2a) bekezdés.
[75] 60/2014. (III. 6.) kormányrendelet, 1. § 4. pont.
[76] 60/2014. (III. 6.) kormányrendelet, 1. § 7. pont.
[77] 60/2014. (III. 6.) kormányrendelet, 1. § 10a. pont.

Felhasznált irodalom

Részletes leírás a CSIRT-csoportok létrehozásáról. Európai Hálózat- és Információbiztonsági Ügynökség, 2006. Elérhető: www.enisa.europa.eu/publications/csirt-setting-up-guide-in-hungarian/at_download/fullReport (a letöltés ideje: 2017.április 15.)

Handbook for CSIRTs. Cert Coordination Center, 2003. Elérhető: http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf (a letöltés ideje: 2017.április 10.)

Incident Handling Management. Európai Hálózat- és Információbiztonsági Ügynökség, 2016. Elérhető: www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/setting-up-a-csirt#Incident_Handling_Management (a letöltés ideje: 2017.április 15.)

GARNAEVA, Maria – SINITSYN, Fedor – NAMESTNIKOV,Yury – MAKRUSHIN, Denis – LISKIN, Alexander (2016): *Kaspersky Security Bulletin: Overall statistics for 2016*. Elérhető: https://kasperskycontenthub.com/securelist/files/2016/12/Kaspersky_Security_Bulletin_2016_Statistics_ENG.pdf (a letöltés ideje: 2017. április 15.)

4. BIZTONSÁGI ESEMÉNYKEZELÉS A NEMZETKÖZI TÉRBEN – A CERT/CSIRT MŰKÖDÉSE

Tikos Anita

4.1. A CERT és a CSIRT fogalma

A informatika robbanásszerű fejlődésének, valamint a digitalizáció térnyerésének köszönhetően egyre több elektronikus szolgáltatás (banki, közigazgatási, elektronikus aláírás, online vásárlás stb.) jön létre, amelyek az életünk minden szegmensében meghatározóvá válnak. A növekvő kitettséggel párhuzamosan egyre jelentősebbé vált az információbiztonság szerepe. Ennek érdekében világszerte számos különböző szervezet, intézmény jött létre, amelyek az információbiztonság elősegítéséért, biztosításáért, megteremtéséért, illetve fenntartásáért felelősek. Ilyen intézmények például a hálózat- és információbiztonsági hatóságok, az eseménykezelő csoportok, a nemzeti kiberbiztonsági központok (National Cyber Security Centers, NCSC), a kiberkiválósági központok, a biztonsági üzemeltetési központok (Security Operation Centers, SOC).

Jelen tananyag az incidens kezelésért felelős, úgynevezett *hálózatbiztonsági eseménykezelő csoportokat* mutatja be, a CSIRT-ek és CERT-ek kialakulását, típusait, feladatait, lehetséges együttműködési modelljeit, valamint a létrehozásuk során megfontolandó főbb kérdéseket tekinti át. A CSIRT és a CERT egyaránt mozaikszavak: a CSIRT a *Computer Security Incident Response Team* (számítógép-biztonsági incidenskezelő csoport) kifejezésből, a CERT pedig a *Computer Emergency Response Team* (számítógépvészhelyzet-kezelő csoport) kifejezésből jött létre.

A CERT, illetve CSIRT egyaránt számítástechnikai vészhelyzetekre reagáló szervezet, amely részt vesz a nemzetközi hálózatbiztonsági vagy kritikus információs infrastruktúrák védelmére szakosodott szervezetek munkájában. Mára már több száz különböző méretű, érettségi szintű CERT és CSIRT működik világszerte.

A CERT kifejezést 1988-ban az Amerikai Egyesült Államokban levédette a CERT Coordination Center (CERT/CC). A CSIRT kifejezés eredetileg az amerikai CERT európai megfelelője, de napjainkban a két kifejezést szinonimaként használjuk.

Egy másik nézet szerint az évek során CERT-szolgáltatások színes spektruma jött létre, ezért egyes szakemberek úgy vélték, hogy nem elég a CERT kifejezés a tevékenységek leírására, ezért az 1990-es évek végén bevezették a CSIRT kifejezést, mely pontosabb képet ad a szervezet által végzett tevékenységről.

A fenti elméletekhez képest teljesen más koncepciót fogalmaz meg a CERT Coordination Center a CERT és CSIRT fogalmak használatáról, miszerint a CERT kifejezés eredetileg ugyan mozaikszóként jött létre, de ma már a Carnegie Mellon Egyetem által levédett és bejegyzett márkanévként kell rá tekinteni. A CERT/CC egyik szolgáltatása, hogy igény esetén lehetővé teszi, engedélyezi – minimális követelmények és szabályok kikötése mellett – a CERT kifejezés használatát más incidenskezelő szervezetek számára is.

A CERT márkát jogosan használó incidenskezelő szervezetek számára a CERT/CC létrehozott egy logót, mely a honlapjukon megjelenítve tanúsítja, hogy a szervezet jogosan használja a CERT-et mint márkát. A CERT kifejezést márkaként jogosan használó szervezetek listája a CERT/CC honlapján elérhető.

1. ábra

A CERT márka logója

Forrás: http://cert.org/incident-management/csirt-development/cert-authorized.cfm (a letöltés ideje: 2017. április 20.)

Tehát a CERT/CC álláspontja szerint, mivel márkajelzésként használandó ez a kifejezés, így nem szabad az incidenskezelésért felelős szervezetek alapvető vagy általános elnevezéseként használni, erre a számítógép-biztonsági incidenskezelő csoport (CSIRT) kifejezést javasolja.

A fentiekből láthatjuk, hogy mindenki által elfogadott, egységesen használt megközelítés vagy definíció egyelőre nem áll rendelkezésünkre. Minden ország vagy nemzetközi szervezet saját maga határozza meg, hogy mit ért pontosan CERT-en vagy CSIRT-en.

Az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (European Union Agency for Network and Information Security, ENISA) 2006-ban a *Részletes leírás a CSIRT-csoportok létrehozásáról*[1] című tanulmányában az alábbiak szerint határozta meg a CSIRT fogalmát: *„A CSIRT olyan információbiztonsági szakemberekből álló csoport, amelynek az az elsődleges feladata, hogy számítógépes biztonsági incidensek esetén beavatkozzon. Biztosítja az ezek kezeléséhez szükséges szolgáltatásokat, és támogatást nyújt vevőinek a rendszerfeltörések utáni helyreállításhoz."*[2]

Jelen tananyagban az incidenskezelésért felelős csoportokra vagy szervezetekre a CSIRT kifejezést használjuk.

4.1.1. Kialakulása

Az első jelentős féregtámadás (worm) a Morris nevű volt a nyolcvanas évek végén. Ez, gyors terjedése miatt, a világ számos rendszerét fertőzte meg. Ezután egyértelművé vált, hogy szükség van olyan szervezetek létrehozására, amelyek ilyen esetekben gyorsan segítséget tudnak nyújtani az informatikusok és rendszergazdák számára, koordinálni tudják az incidensek kezelését és a különböző érintett szervezetek szakembereinek együttműködését.

Ezért a Morris féreg támadását követő napokban, 1988-ban Pittsburgh-ben, a Carnegie Mellon Egyetemen létrehozták az első CERT-et, CERT Coordination Center – CERT/CC (CERT Koordinációs Központ) néven.

Ezt követően sorra jöttek létre hasonló, incidenskezelésért felelős szervezetek különböző szervezeti elnevezésekkel, mint például CSIRT, CIRT (*Computer Incident Response Team*), IRT (Incident Response Team), illetve SERT (*Security Emergency Response Team*) nevű szervezetek.

Az Egyesült Királyságban úgynevezett WARP-okat (Warning, Advise and Reporting Points) hoztak létre. A WARP-ok részét képezik az Egyesült Királyság IT-biztonságát szavatoló, valamint a nemzeti kritikus infrastruktúra védelméért felelős szervezetrendszernek. Feladatuk a sérülékenységekről szóló információk gyűjtése és megosztása, riasztások kiadása (*warning*), a jó gyakorlatok megosztása (*reporting*), továbbá szükség esetén segítségnyújtás, tanácsadás (*advise*). Ezen szervezetek

---

1 www.enisa.europa.eu/publications/csirt-setting-up-guide-in-hungarian/at_download/fullReport (a letöltés ideje: 2017. április 20.)

2 *Részletes leírás a CSIRT-csoportok létrehozásáról.* Elérhető: www.enisa. europa.eu/publications/csirt-setting-up-guide-in-hungarian/at_download/fullReport (a letöltés ideje: 2017.április 15.)

létrehozása elősegíti az incidensekről és sérülékenységekről szóló információk megosztását, de jóval egyszerűbb és olcsóbb megoldás, mint különböző CSIRT-eket létrehozni.

Az internetszolgáltatók körében az úgynevezett *Abuse Team*-ek látnak el a CSIRT-ekhez hasonló funkciókat. Főbb feladatuk a kisebb, szinte mindennapos incidensek kezelése (például spamek, adathalászat).

Európában az első CSIRT 1992-ben jött létre, a SURFnet holland egyetemi szolgáltatónál, SURFnet-CERT néven. Számos CSIRT alakult az elmúlt évek során a világ minden részén, különböző területeken különböző szolgáltatásokkal és képességekkel. Az ENISA 2006-os nyilvántartása alapján Európában több mint 100 CSIRT létezett.

4.1.2. CSIRT-típusok

Többféle CSIRT-et különböztethetünk meg aszerint, hogy az adott szervezet milyen területen, szektorokban végzi tevékenységét, nyújtja a szolgáltatásait. Szinte minden országban működik nemzeti CSIRT, kormányzati CSIRT, kritikus infrastruktúra CSIRT, egyetemi CSIRT, katonai CSIRT, esetleg ezek tetszőleges kombinációja (bizonyos esetekben egy adott CSIRT több különböző típusú CSIRT funkcióját is ellátja).

Ezeken kívül világszerte számos szektorális (energia, bank, közlekedés) CSIRT is létrejött. A nagyobb cégeknél a cégen vagy cégcsoporton belül előfordul, hogy létrehoznak a saját rendszereik és szolgáltatásaik számára saját, úgynevezett belső CSIRT-et. Ezen kívül vannak még úgynevezett üzleti és szoftverkiadó CSIRT-ek is.

Nemzeti CSIRT

A nemzeti CSIRT különlegesnek tekinthető abban a tekintetben, hogy fő feladata a koordináció az adott ország eseménykezelő csoportjai között, valamint úgynevezett kapcsolattartó feladatkör betöltése nemzeti és nemzetközi szinten egyaránt. Nemzeti CSIRT szinte minden országban van, de ezek minden esetben különböző szerepet töltenek be. A legfontosabb, hogy egyetlen, mindenki által (nemzetileg és nemzetközileg) ismert kapcsolattartóként működjön, így ha egy incidens esetén az érintett nem tudja, hogy kihez kell fordulni, mely CSIRT a felelős az adott kérdésben, akkor a nemzeti CSIRT-hez tud fordulni segítségért, tájékoztatásért.

A nemzeti CSIRT-ek nyilvántartják az országban működő CSIRT-eket, a képességeiket és elérhetőségeiket, jó gyakorlatokat tesznek közzé, az információbiztonsági oktatásban és tudatosításban vezető szerepet vállalnak, a nemzetközi közösségekből érkező értesítések vagy technikai elemzések fordítását megosztják a nemzeti CSIRT-közösséggel, valamint segítenek az országon belül CSIRT-ek létrehozásában vagy fejlesztésében.

Kormányzati CSIRT

A kormányzati CSIRT a kormányzat és az egyéb állami szervezetek informatikai biztonságának kialakítását segíti elő, valamint segítséget nyújt incidensek esetén. Egyes országokban az állami és kormányzati rendszerek és eszközök biztonságán túl az állampolgárok és adataik biztonságáért vagy a kritikus információs infrastruktúra védelméért is felelős lehet.

A nemzeti és kormányzati CSIRT-ek kiemelt fontosságúak minden országban a többi eseménykezelő csoporthoz képest; számos plusz feladattal rendelkeznek, amelyek a nemzeti szintű koordinációt hivatottak megvalósítani.

Számos esetben a kormányzati CSIRT látja el a nemzeti CSIRT-ek feladatainak egy részét, vagy a kormányzati CSIRT egyben nemzeti CSIRT-ként is funkcionál.

Katonai CSIRT (MILCERT)

A katonai CSIRT-ek az ország katonai, honvédelmi szervezeteinek, az ország védelmi infrastruktúráinak nyújtanak CSIRT-szolgáltatásokat. Katonai nemzetközi együttműködésekben, információbiztonsági közösségekben vesznek részt.

Kritikus infrastruktúra CSIRT

Kifejezetten a kritikus információk és infrastruktúrák védelméért felelős CSIRT-ek is léteznek számos országban. Tulajdonképpen a legfőbb szektorok (energia, közlekedés stb.) kulcsfontosságú infrastruktúrájának védelméért, így pedig közvetve az állampolgárok biztonságáért is felelős a Kritikus infrastruktúra CERT (CIP CSIRT vagy CIIP CSIRT).

Egyetemi vagy akadémiai CSIRT

A tudományos szektorban, egyetemeken, kutatóintézetekben szokták létrehozni. Feladata az adott oktatási, kutatási intézmény elektronikus rendszereinek védelme. Számos esetben hoznak létre labort a CSIRT-en belül, amely lehetővé teszi a kiberbiztonsági gyakorlatok és tesztek lebonyolítását is. A tudományos területen működő CSIRT jó lehetőség a kiemelkedő eredményeket felmutató tanulók bevonására, továbbfejlesztésére egyaránt.

Üzleti CSIRT

Általában egy bizonyos szektorra, területre (például internetszolgáltatók) specializálva, üzleti alapon nyújt CSIRT-szolgáltatásokat. Ez esetben ez a szervezet maga is a piac részét képezi, a szolgáltatásokból kapott bevételből tartja fenn magát.

Belső CSIRT

A belső CSIRT-et általában egy adott cégen vagy cégcsoporton belül hozzák létre, szolgáltatásait főként az anyaszervezetnek és a cégcsoport tagjainak nyújtja. A legtöbb esetben bankok és telekommunikációs szervezetek esetében figyelhetjük meg belső CSIRT létrehozását, működését.

A belső CSIRT-ekről a nyilvánosság számára általában nem érhető el semmilyen információ, nincs publikus honlapjuk, leírásuk, elérhetőségük. Ezen típusú eseménykezelő csoportok főként a szektorban működő egyéb CSIRT-ekkel, a nemzeti vagy kormányzati CSIRT-ekkel vannak szoros együttműködésben, valamint a szektorban működő eseménykezelő közösségek munkájában vesznek részt.

Szoftverkiadó CSIRT

Az ilyen típusú CSIRT általában egy adott szoftverkiadó termékeinek támogatására jön létre. A termékek sérülékenységeinek, sebezhető pontjainak kiküszöbölése, megoldása a feladata.

4.2. A CSIRT-ek feladatai, szolgáltatásai

Kezdetekben a CSIRT-eknek csupán az incidensekre való reagálás, úgynevezett *eseti, készenléti beavatkozás* volt a feladatuk. Idővel folyamatosan fejlesztették képességeiket és szolgáltatásaikat az aktuális kihívásoknak megfelelve, valamint egy adott terület vagy szektor igényeihez igazodva. Így mára a CSIRT feladatai közé tartozik a riasztások kiadása, az oktatás, a tudatosítás, a biztonságkezelés egyaránt.

A CSIRT-ek a feladataikat több különböző szolgáltatás útján látják el. Az eseménykezelő csoportok annyira sok, különböző szolgáltatással rendelkeznek, hogy egyelőre még nem volt arra példa, hogy egy CSIRT minden szolgáltatást nyújtani tudott volna. A CERT Competence Center készített egy átfogó összefoglalást a lehetséges szolgáltatásokról a CSIRT-ek számára megfogalmazott kézikönyvben. A legtöbb szakirodalom ezt az összefoglalót veszi alapul a szolgáltatások áttekintéséhez, ezért a jelen tananyag is ezt használja.

1. táblázat

A CSIRT-ek különböző szolgáltatásai

Megelőzést nyújtó szolgáltatások	Válaszintézkedést nyújtó szolgáltatások	Biztonsági minőségirányítás
• *Riasztások és figyelmeztetések* • *Incidenskezelés* Incidenselemzés Incidenssel kapcsolatos helyszíni válaszintézkedések Incidenssel kapcsolatos válaszintézkedések koordinálása • *Sebezhetőség kezelése* Sebezhetőség elemzése Sebezhetőséggel kapcsolatos válaszintézkedések Sebezhetőséggel kapcsolatos válaszintézkedések koordinálása • *Kártékony kódok kezelése* Kártékony kódok elemzése Kártékony kódokkal kapcsolatos intézkedések Kártékony kódokkal kapcsolatos intézkedések koordinálása	• *Bejelentések* • *Technológiafigyelés* • *Biztonsági ellenőrzések és felmérések* • *Biztonsági konfiguráció beállítása és karbantartása* • *Biztonsági eszközök fejlesztése* • *Behatolásérzékelési szolgáltatások* • *Biztonsággal kapcsolatos információk terjesztése*	• *Kockázatelemzés* • *Üzletmenet- folytonosság és katasztrófa utánivisszaállítás* • *Biztonsági tanácsadás* • *Tudatosság növelése* • *Oktatás/képzés* • *Termék kiértékelése vagy tanúsítása*

Forrás: Handbook for CSIRTs. (2003). http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf (a letöltés ideje: 2017. április 1.)

A válaszintézkedést nyújtó szolgáltatások és a megelőző szolgáltatások egy részét (riasztások és figyelmeztetések, incidenskezelés, incidenselemzés, incidenssel kapcsolatosan tett válaszintézkedések támogatása, illetve koordinálása, bejelentések) úgynevezett *alapvető szolgáltatásoknak* nevezzük, mert tulajdonképpen ezek képezik egy CSIRT főbb feladatait.

4.2.1. Válaszintézkedést nyújtó szolgáltatások (reaktív szolgáltatások)

A válaszintézkedésre fókuszáló feladatok célja, hogy a CSIRT ügyfélköréhez tartozó szervezetektől, ügyfelektől érkező incidensbejelentésre, valamint a CSIRT rendszereit érintő fenyegetésre vagy támadásra vonatkozó válaszintézkedés, reagálás, valamint az általuk okozott kár enyhítése megtörténjen.

A *riasztások és figyelmeztetések* a behatolási szándékú támadásra, a sebezhetőségekre, a vírusokra, valamint az álriasztásokra vonatkozó információk terjesztését jelenti az ügyfélkör számára. A kiküldött riasztás vagy figyelmeztetés tájékoztatja az ügyfélkört egy adott sérülékenységről, továbbá tartalmazhat útmutatást a rendszereik megvédéséhez, valamint javaslatot a probléma kezelésére.

Az *incidenskezelési feladatot* a CSIRT-ek különböző módon valósíthatják meg. Vannak követhető incidenskezelési szabványok (NIST, ISO27000 szabványcsalád), illetve számos incidenskezelési útmutatót készítettek különböző CSIRT-ek és tanácsadó szervezetek (például az ENISA), amelyek hasznosak és követhetőek az incidenskezelés folyamatának kialakítása során.

Az incidenskezelés folyamatába a bejelentések fogadása, priorizálása, a válaszintézkedések megfogalmazása, az incidensek elemzése tartozik. Esetenként a bírósági bizonyítékok gyűjtése, illetve a behatoló rendszeren belüli tevékenységének nyomon követése is beletartozhat ebbe a folyamatba.

A CSIRT-ek *helyszíni segítségnyújtást* is végezhetnek az ügyfél kérése esetén. Ez esetben a CSIRT munkatársai végzik a helyszínen a rendszer fizikai elemzését, javítását és helyreállítását egyaránt. Ide tartozik minden olyan lehetséges tevékenység, amit egy incidens gyanúja vagy megvalósulása miatt javasolt elvégezni.

Az *incidenssel kapcsolatos válaszintézkedések támogatása* szolgáltatás keretében a CSIRT egy sérülékenység vagy incidens esetén az ügyfélnek telefonon vagy e-mailben nyújt segítséget, ad tanácsot a helyreállításhoz. Ide értendő az összegyűjtött adatok technikai elemzésében történő segítségnyújtás, kapcsolattartás, a kárcsökkentési és helyreállítási stratégiák javaslata. Ez a helyszíni válaszintézkedéstől annyiban tér el, hogy ez esetben a helyszíni feladatokat az ügyfél rendszergazdái látják el a mindennapi feladatuk részeként, a CSIRT-tel való szoros együttműködésben, a CSIRT útmutatásai alapján.

Az *incidenssel kapcsolatos válaszintézkedések koordinálása* során a CSIRT több érintett fél között koordinál, és segítséget nyújt a támadásban érintett áldozat és az egyéb érintett „helyszínek” számára. A gyakorlatban ez azt jelenti, hogy ha az incidensben érintett ügyfélen túl az internetszolgáltatók, valamint más CSIRT-ek bevonása is szükséges az incidens kezelésébe, akkor a CSIRT koordinálja a különböző érintettek feladatait, és közvetít a felek között.

A koordinációs feladat a kapcsolattartási információk gyűjtéséből, az érintettek értesítéséből, statisztikák gyűjtéséből, elemzések támogatásából, szükség esetén az ügyfél jogi vagy kommunikációs területével való kapcsolattartásból áll. Helyszíni támogatást, intézkedést nem foglal magában. Bizonyos esetekben szükség van a rendőrség bevonására is, ha egy incidensnél felmerül a bűncselekmény lehetősége. Ekkor a CSIRT a rendőrséggel való koordinációt is végezheti.

A *sebezhetőség kezelése* a hardverek és szoftverek sérülékenységéről szóló jelentések, tájékoztatások fogadására, a sebezhetőség jellegének, működésének és lehetséges hatásainak elemzésére terjed ki, valamint stratégiák kidolgozására, annak észlelésére, valamint megszüntetésére.

A tapasztalatok alapján a CSIRT-ek különböző módon és mértékben valósítják meg a sebezhetőség kezelésére vonatkozó feladatot.

A *sebezhetőség elemzése* a szoftver- és hardversebezhetőségek műszaki elemzését jelenti. Az elemzés célja a feltételezett sebezhetőség ellenőrzése, valamint a sebezhetőség helyének és lehetséges felhasználásának felderítése. Ennek az egyik módja lehet például az úgynevezett forráskódhibakereső program használata.

A *sebezhetőséggel kapcsolatos válaszintézkedések* a sebezhetőség megszüntetésére irányulnak, amelyet javítóprogramok, hibajavító frissítések és egyéb átmeneti megoldások kidolgozása útján valósít meg a CSIRT. E feladat részét képezik a kárcsökkentő megoldások és stratégiák kommunikálása, a riasztások kiadása.

A *sebezhetőséggel kapcsolatos válaszintézkedések koordinálása* során a CSIRT értesíti az érintett szervezeteket vagy a szervezeten belüli részlegeket a sebezhetőségről, valamint a sebezhetőség csökkentésére, javítására javaslatokat tesz. Ezt követően akár még ellenőrizheti is a sebezhetőség megszüntetésének megvalósulását. Ez a szolgáltatás kiterjedhet a sebezhetőség elemzésére, a különböző érintett felek (áldozatok, szolgáltatók, CSIRT-csoportok, ügyfelek, szakemberek) elemzéseinek összehasonlítására, összegzésére, az érintett felek közötti kommunikáció koordinálására.

Az ilyen feladatot ellátó CSIRT-ek nyilvántartást vezethetnek a különböző megvalósult sebezhetőségekről és az azokra vonatkozó válaszstratégiákról.

A *kártékony kódokat* a korábbi elemzésekben külön (4.) szolgáltatási csoportként tüntették fel. Olyan szolgáltatások tartoznak ide, melyek feladata a rendszer azon elemeinek, fájljainak elemzése,

amelyek bármilyen módon szerepet játszhattak az adott sérülékenység kialakulásában, az incidens megvalósulásában (például vírusok, férgek, egy-egy sebezhetőséget kihasználó szkript). Abban az esetben, ha ez a folyamat valamilyen program vagy szoftver hibájára mutat rá, akkor erről a CSIRT tájékoztatja a szoftverkiadó CSIRT-et, a szoftver fejlesztőit, illetve az egyéb lehetséges érintetteket (esetleg CSIRT-közösségeket). Ez már az alapvető CSIRT-feladatokon túlmutat, célja a probléma kijavítása, a további incidensek megelőzése, a kockázatok csökkentése.

A kártékony kódokról szóló információkat, az illetéktelen behatoláshoz vagy kárt okozó tevékenységhez kapcsolódó kártékony kódokról készült másolatokat megkaphatják a CSIRT-ek, amelyek a kapott adatokat és információkat megvizsgálják. A vizsgálat kiterjedhet a kártékony kódok jellegének, működésének és alkalmazásának elemzésére. Ezt követően dolgozzák ki a kártékony kódok észlelésére, eltávolítására vagy megelőzésére vonatkozó javaslatokat, stratégiákat.

A *kártékony kódok kezelése* az incidensbejelentéshez hasonló abban a tekintetben, hogy a CSIRT-ek különböző módon valósítják meg, így a kártékony kódok kezelésébe az elemzés, a kártékony kódokkal kapcsolatos intézkedések vagy azoknak koordinálása tartozhat bele.

A *kártékony kódok elemzése* a rendszerben talált kártékony kódok műszaki vizsgálatát és elemzését, felépítésének (például fájlrendszerek, alkalmazott fájltípusok) feltárását jelenti. Azonosítja, hogy mi volt a célja és feladata a torzulásnak. Ebbe beletartozik az is, hogy a CSIRT összeveti az aktuálisan vizsgált kártékony kódokat a már ismert kártékony kódokkal, azonosítja az eltéréseket és hasonlóságokat.

A *kártékony kódokkal kapcsolatos intézkedéseken* belül a CSIRT a kártékony kódok telepítésének megakadályozását, a kártékony kódok észlelését és a rendszerből történő eltávolítását célzó tevékenységeket végez vagy határoz meg. Ezen *intézkedések koordinálás*ára vonatkozóan két tevékenységet foglalhat magába ez a szolgáltatás. Egyrészt jelentheti a különböző forrásokból származó eredmények és műszaki elemzések összegzését, másrészt pedig a kártékony kódok elemzési eredményeinek és az arra vonatkozó válaszstratégiáknak megosztását más CSIRT-csoportokkal és biztonsági szakértőkkel. A tevékenység részét képezheti még a kártékony kódok hatásait és a lehetséges válaszintézkedéseket magában foglaló nem nyilvános archívum létrehozása is.

4.2.2. Megelőző szolgáltatások

A megelőző szolgáltatások arra koncentrálnak, hogy az incidensek bekövetkezése előtt javítsanak a rendszeren és a biztonsági folyamatokon, intézkedéseken. Abban az esetben, ha az incidens mégis bekövetkezik, akkor az a célja a megelőző szolgáltatásoknak, hogy az eseményeknek minél kisebb károkozási képessége lehessen.

A *bejelentés* az alapvető CSIRT-feladatok vagy -szolgáltatások közé tartozó egyetlen megelőző szolgáltatás. Ennek során a CSIRT riasztások, tájékoztatások útján figyelmezteti az ügyfeleit az új sebezhetőségekről, a behatoláshoz használható eszközökről. Így az ügyfelek el tudják kerülni ezen sérülékenységeket a rendszerük megfelelő védelmével.

A *technológiai figyelés* során a CSIRT-ek nyomon követik az új informatikai fejlesztéseket és a számítógépes bűnözők tevékenységeit a jövőbeli lehetséges fenyegetések mielőbbi felismerése érdekében. Ennek része a különböző informatikai és információbiztonsági tudományos, műszaki, jogi és politikai hírek, szakmai cikkek és weboldalak nyomon követése.

A technológiai figyelés lehetséges eredményei lehetnek az új kihívásokra vagy fenyegetésekre vonatkozó információkat összegző anyagok, valamint útmutatók, javaslatok a fenyegetés elkerülésére.

A *biztonsági ellenőrzések és felmérések* során a CSIRT az ügyfél biztonsági infrastruktúráját vizsgálja, ellenőrzi, hogy az megfelel-e a szervezet biztonsági szabályainak, valamint az ipari szabványoknak, előírásoknak. Több különböző ellenőrzést vagy felmérést lehet ezen a szolgáltatáson belül biztosítani, attól függően, hogy mi az ellenőrzés pontos célja:

- Az infrastruktúra felülvizsgálata: hardver-, szoftverkonfigurációk, tűzfalak, asztali eszközök és kiszolgálók vizsgálata a biztonsági szabályzat és az ipari szabványos konfigurációk alapján.
- A legjobb gyakorlat vizsgálata: a CSIRT munkatársai azt vizsgálják, hogy a mindennapok során alkalmazott biztonsági intézkedések, gyakorlatok megfelelnek-e a szervezet biztonsági szabályainak, valamint az egyéb kötelező szabályoknak, szabványoknak.
- Gyenge pontok keresése: a CSIRT sebehetőség- és víruskeresők segítségével fedi fel a vizsgált rendszer gyenge pontjait.
- Penetrációs teszt: behatolás vizsgálat, betörésteszt. Egy olyan eljárás, mely során a CSIRT értékeli az ügyfél informatikai infrastruktúráját, védelmi mechanizmusainak hatékonyságát, valamint feltárja a rendszer sérülékenységeit, mint például az operációs rendszerek vagy szolgáltatások hibáit, a nem megfelelő konfigurálást vagy a kockázatos felhasználói viselkedéseket. A behatolásvizsgálatot az ügyfél rendszerei és hálózatai ellen indított szándékos támadás útján végzik.

A nem alapvető, megelőző CSIRT-szolgáltatások színesítik, erősítik egy adott CSIRT képességeit. Általában az alapvető szolgáltatások bevezetését követően, az ezeket használó kör igényei szerint dönti el az adott CSIRT, hogy a fentiek közül melyekkel egészítse ki a szolgáltatásainak körét.

4.2.3. Biztonságkezelési és minőségirányítási szolgáltatások

A biztonságkezelési és minőségirányítási CSIRT-szolgáltatások hosszabb távú célok megvalósítására hivatottak. Főként tanácsadást és oktatást tartalmazó tevékenységek, feladatok tartoznak ide.

A *kockázatelemzés* során a CSIRT a rendszerek és az üzleti folyamatok áttekintésével segít az ügyfélnek reálisan felmérni kulcsfontosságú rendszereit és az azokra irányuló fenyegetettségeket, valamint ezek károkozási képességeit. Az elemzés eredményterméke rámutat, mely rendszerelemek védelmi intézkedéseit érdemes javítani, hogy azok eleget tegyenek a kockázatarányos védelmi képességnek. Egyes CSIRT-ek a teljes kockázatelemzést maguk végzik, míg mások ahhoz csak segítséget nyújtanak az ügyfélnek.

Az üzletmenet-folytonosság biztosítása és a katasztrófa utáni visszaállítás tervezése egyre fonosabb feladat, hiszen a cégek üzleti tevékenységét növekvő mértékben támogatják az informatikai rendszerek. Alapvető érdeke minden szervezetnek, hogy a folyamatait zavartalanul és biztonságosan tudja működtetni. A legnagyobb körültekintés mellett is előfordulhatnak olyan előre nem látható események, amelyek képesek jelentősen lassítani vagy akár teljesen megbénítani ezen folyamatokat. A zavartalan működést úgy tudjuk a legrövidebb idő alatt visszaállítani, ha preventív eljárásokat dolgozunk ki rájuk, és azokat rendszeresen teszteljük. Ennek biztosítása érdekében a tervezés folyamán fontos figyelembe venni az incidensekre és biztonsági eseményekre adott és adható legjobb válaszintézkedést. Erre vonatkozóan a CSIRT-eknek sok tapasztalata és információja van, amit érdemes figyelembe venni. Az ilyen tanácsadási szolgáltatást is nyújtó CSIRT-eket az üzletmenet-folytonossági és a katasztrófa utáni visszaállítási tervek információbiztonsági vonatkozású részeinek kidolgozásába is be szokták vonni.

A *biztonsági tanácsadással* foglalkozó CSIRT-ek ezen szolgáltatás körében az ügyfelére, valamint az ügyfél vevőkörére vonatkozó biztonsági szabályzatok elkészítéséhez nyújtanak segítséget, illetve felülvizsgálják a már elkészült szabályzatokat. A tanácsadás kiterjedhet például az ügyfél új rendszereinek, vállalati folyamatainak vagy eszközeinek biztonságossá tételére vagy akár a biztonságos telepítéssel kapcsolatos követelmények, szabályok leírására is.

Az emberi tényező szerves része az informatika rendszerek működésének, biztonságának, hiszen a munkatársak adatokat rögzítenek, feldolgoznak, leveleket fogadnak, továbbítanak stb. Számos fenyegetés egyenesen a felhasználót veszi célba, és ezek fő célja, hogy annak jóhiszeműségére vagy képzetlenségére támaszkodva kárt okozzon. Ezért elengedhetetlen a felhasználók képzése, hogy meg tudják különböztetni a rosszindulatú fenyegetést a valós kérésektől. A *tudatosság növelése* nagyban

hozzájárul ahhoz, hogy az ügyfél munkatársai biztonságosabban tudják végezni mindennapi munkájukat, amelynek köszönhetően csökken az ügyfél és rendszerei elleni sikeres támadások száma is.

Az ilyen szolgáltatást nyújtó CSIRT-ek a tudatosság növelésének számos formáját, eszközét használják tevékenységük során, hogy az ügyfél minden munkatársának el tudják magyarázni a legjobban bevált biztonsági gyakorlatokat, valamint a szükséges óvintézkedéseket és azok fontosságát. A CSIRT-ek ezen cél érdekében cikkeket, plakátokat, infografikát, hírleveleket készítenek vagy akár szemináriumokat szerveznek.

Az *oktatás, képzés* keretein belül a CSIRT szemináriumokat, tanfolyamokat, konzultációkat tart az ügyfelei számára az informatikai biztonsági kérdésekről. Ez a szolgáltatás már az általános tudatosság növelésnél konkrétabb, speciálisabb témákat érint, mint például az incidens bejelentésére vonatkozó útmutatás, az incidensészlelés, a lehetséges válaszintézkedések és az ahhoz használandó eszközök, valamint az incidens-megelőzési módszerek.

A *termékértékelés vagy a tanúsítás* során a CSIRT-ek – tevékenységük részeként – eszközök, alkalmazások és szolgáltatások vizsgálatát, sőt akár tanúsítását is elvégezhetik. Ez esetben a cél a termék biztonságosságának, valamint a szervezet biztonsági szabályzatának való megfelelés biztosítása. Azon CSIRT-ek, amelyek rendelkeznek valamilyen tanúsítói jogkörrel, az értékelésen túl tanúsítással is elláthatják a vizsgált eszközt vagy szolgáltatást.

4.2.4. Az európai uniós szabályozás által definiált CSIRT-feladatok

A 2013-as európai uniós kiberbiztonsági stratégiának és a 2016-ban elfogadott hálózat- és infomációbiztonsági irányelvnek (NIS)[3] egyaránt az az alapvető célja, hogy minden tagállam azonos minimumképességekkel, jogszabályi háttérrel, reagálási képességgel és szervezeti rendszerrel rendelkezzen. Ennek megfelelően a NIS-irányelv 9. cikke úgy rendelkezik, hogy minden európai uniós tagállamnak ki kell jelölnie egy vagy több CSIRT-et legalább az irányelv hatálya alá eső ágazatokban és szolgáltatásokban. Az irányelv a CSIRT-ekre vonatkozóan konkrét kötelezettségeket és feladatokat fogalmaz meg az I. mellékletben. Ez tulajdonképpen azt jelenti, hogy a NIS-irányelv hatálya alá tartozó szektorokban a kockázatok és biztonsági események kezeléséért felelős, számítógép-biztonsági eseményekre reagáló csoportoknak legalább az irányelv mellékletében szereplő feladatokat el kell látniuk.

Az irányelv elsőként azon kritériumokat fogalmazza meg, amelyekre szükség van ahhoz, hogy a CSIRT a feladatait folyamatosan és megfelelően el tudja látni. Ezt az irányelv a CSIRT kötelezettségeinek nevezi:

- a hírközlési szolgáltatások magas rendelkezésre állása (7/24-es elérhetőség),
- az egyértelműen definiált kommunikációs csatornák,
- a CSIRT-et és annak informatikai rendszereit biztonságos helyszínen kell elhelyezni,
- gondoskodni kell az üzletmenet-folytonosságról,
- a nemzetközi együttműködési hálózatokban való részvétel.

Az irányelv alapján a CSIRT-ek feladatai:

- a biztonsági események monitorozása nemzeti szinten,
- a kockázatok vagy biztonsági események korai előrejelzése, riasztások kiküldése, valamint az információk továbbítása, terjesztése az érdekelt feleknek,
- a biztonsági eseményre való reagálás (úgynevezett incidenskezelés),
- a kockázat- és eseményelemzés,
- a helyzetkép elkészítése,
- a CSIRT-ek hálózatában való részvétel,

[3] *NIS-irányelv.* Elérhető: http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.HUN&toc=OJ:L:2016:194:TOC (a letöltés ideje: 2017. április 20.)

- együttműködés kialakítása a magánszféra szereplőivel,
- a közös szabványosított eljárások alkalmazása a biztonsági események és kockázatok kezelésére,
- a közös szabványosított eljárások alkalmazása a biztonsági események, kockázatok és információk osztályozására szolgáló rendszerekben.

Az irányelv által definiált minimális -feladatok tulajdonképpen egybeesnek a CERT/CC által megfogalmazott alapvető CSIRT-szolgáltatásokkal, -feladatokkal.

4.3. Az incidenskezelés hátterének megismerése

Már említettük, hogy számos ajánlás és jó gyakorlat jött létre az incidenskezelés folyamatáról. Ennek a tananyagnak nem képezi részét az incidenskezelés folyamatának és módszertanának áttekintése, ezért most csak a főbb ajánlások, jogszabályok és szabványok rövid bemutatására kerül sor.

Az incidenskezelésről megfelelő áttekintést nyújt a CERT/CC által a CSIRT-ek létrehozásához készített kézikönyv,[4] vagy az egyéb, az incidenskezelés, incidensmenedzsment témában készített publikációk (például a fehér könyv az incidensmenedzsmentről).[5]

Vannak olyan anyagok is, amelyek kifejezetten egy szűk célközönség számára készültek, ilyen például a SANS intézet által kiadott, kis- és középvállalkozásoknak szóló incidenskezelési útmutató.[6]

4.3.1. Az ENISA

Az ENISA egyik kiemelt feladata az EU-s tagállamok eseménykezelő központjainak való tanácsadás és segítségnyújtás. Ez az incidenskezelés vagy más néven incidensmenedzsment kérdéskörében is megmutatkozik: számos tanulmányt, összefoglalót sőt, tananyagot találhatunk az ENISA honlapján ebben a témakörben. A 2006-ban készült, *Részletes leírás a CSIRT-csoportok létrehozásáról* című tanulmánynak is része az incidenskezelés folyamata, de az ENISA-nak vannak kifejezetten ezzel a témával foglalkozó összefoglalói, útmutatói, tananyagai is. 2010-ben készítettek egy útmutatót az incidensmenedzsment jó gyakorlatairól.

Az ENISA feladatai között szerepel a képzések és tréningek biztosítása, melyekben természetesen az incidenskezelés témaköre is helyet kapott. A CSIRT-ek létrehozásáról szóló képzés része az incidenskezelés is, amelynek képzési tananyagai közé 2016-ban került be a megújított, úgynevezett incidenskezelés-menedzsment kézikönyv.[7]

Ezenkívül számos egyéb, az incidenskezelés egyes területeire koncentráló képzési anyag is található az ENISA képzési kínálatában, mint például az incidenskezelés a felhőben, nagyméretű, jelentős incidensek kezelése, a kritikus infrastruktúrákat érő támadások során az incidensek kezelése, az adathalászkampány során alkalmazandó incidenskezelés és együttműködés, illetve mobilfenyegetések során alkalmazandó incidenskezelés témákban.

---

[4] *Handbook for CSIRTs.* Elérhető: http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf (a letöltés ideje: 2017. április 20.)

[5] *Incident management White paper.* Elérhető: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=295919 (a letöltés ideje: 2017. április 20.)

[6] *Incident handling process for small and medium businesses.* Elérhető: www.sans.org/reading-room/whitepapers/incident/incident-handling-process-small-medium-businesses-1791 (a letöltés ideje: 2017. április 20.)

[7] *Incident handling management.* Elérhető: www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/setting-up-a-csirt#Incident_Handling_Management (a letöltés ideje: 2017. április 20.)

4.3.2. Az Information Technology Infrastructure Library (ITIL)

Az ITIL egy informatikai rendszerek üzemeltetésére és fejlesztésére vonatkozó ajánlás, módszertan, amely az Egyesült Királyság szabványosító tevékenysége során jött létre és vált nemzetközi szabvánnyá. Az ITIL csomagjából a 3. verzió, az úgynevezett ITILv3 a legfrissebb. Ez az ajánláscsomag tulajdonképpen 5 fő kötetből, illetve a hozzájuk kapcsolódó kiegészítő anyagokból áll, melyek az incidenskezelés témakörére is kiterjednek. A szolgáltatásüzemeltetésről szóló kötet a szolgáltatás folytonosságához, az információbiztonság menedzsmentjéhez, a hibamentes üzemeltetéséhez szükséges folyamatokat tartalmazza, a melynek az egyik fontos eleme az incidenskezelés.

4.3.3. A Control Objectives for Information and Related Technologies (Cobit)

Az ISACA információs rendszer menedzserek és ellenőrök nemzetközi szakmai szervezete, amelynek összesen 180 országban nagyjából 140 000 tagja van. A szervezet célja a jó gyakorlatok felkutatása, oktatása és világszinten történő elterjesztése. Az ISACA által tárgyalt témák közé tartozik az információbiztonság és az incidenskezelés egyaránt. Információbiztonsági témájú anyagai közül az incidenskezelésre való tekintettel kiemelendő a *Cobit 5 for Information Security* című, átfogó információbiztonsági koncepciót tartalmazó anyag, valamint a biztonsági eseménykezelés vizsgálati programja, amely eredetileg az eseménykezelés folyamatának felmérésére és értékelésére szolgál, de nemcsak a már meglévő szolgáltatásuk értékelésekor lehet hasznos, hanem a szolgáltatás kidolgozásakor is megfontolandó szempontokat, kritériumokat tartalmaz.

4.3.4. National Institute of Standards and Technology (NIST)

Az Amerikai Egyesült Államok Nemzeti Szabvány és Technológiai Intézete (NIST) az egyik legismertebb szabványosítással foglalkozó szervezet a világon, amely az információs technológiákon belül az információbiztonság területén is készít kiadványokat. 2013-ban kiadta a *kiberbiztonsági keretirányelvet,* mely az incidensmenedzsmentre is kiterjed, valamint összefoglalja a figyelembe veendő szabványokat.

2012-ben megjelentette az SP800-61 számú számítógépes biztonsági eseménykezelési útmutatót, később pedig a NIST SP 800-53 számú kiadványt, ami tulajdonképpen a biztonsági kontrollokat tartalmazó gyűjtemény, amelyen belül az IR4 kifejezetten az incidenskezelésről szól.

4.3.5. Az ISO 27000-es szabványcsalád

A NIST szabványügyi szervezet létrehozta a 27000-es számú szabványcsaládot, mely az információbiztonság és menedzselése területre vonatkozó szabványokat foglalja magában. Ezen szabványcsalád alapjait az 1990-es években létrejött brit információbiztonsági szabványok (BS7799-1 és BS7799-2) jelentették.

A szabványcsalád részeként jött létre az ISO/IEC 27035:2011 számú, a biztonsági incidenskezelésről szóló szabvány, amely a biztonsági eseménykezelés gyakorlatait foglalja össze.

4.3.6. Jogalkotás

Európai uniós szinten a *Hálózat- és információbiztonsági irányelv,* Magyarországon pedig a Kormányzati Eseménykezelő Központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának

és a sérülékenységvizsgálat lefolytatásának szabályairól szóló, 185/2015. (VII. 13.) számú kormányrendelet fogalmazza meg a főbb szabályokat, alapelveket az incidenskezelésről.

4.4. A CSIRT-ek Magyarországon

Magyarországon az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) teremtette meg a kibertér védelmének, az információbiztonság alapjainak jogi kereteit, valamint létrehozta a magyarországi kibervédelmi szervezetrendszert. Ennek megfelelően a törvény számítógépes eseménykezelő központok létrehozását és működtetését is előírja.

Az Ibtv. a számítógépes eseménykezelő központokról a korábbi ENISA-ajánlásban szereplő definíciót vette át, miszerint a CSIRT tulajdonképpen olyan számítástechnikai vészhelyzetekre reagáló egység, mely tagsággal és akkreditációval rendelkezik a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben. A CSIRT definíciójának részét képezi a törvényben a CSIRT és a CERT fogalmának elhatárolása. E tekintetben a törvény azt a nézetet képviseli, hogy a CERT az amerikai, a CSIRT pedig az európai elnevezése a számítógépes eseménykezelő központoknak.

Az Ibtv. előírja a Kormányzati Eseménykezelő Központ (GovCERT) működtetését, valamint lehetővé teszi ágazati eseménykezelő központok létrehozását is.

A kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól szóló 185/2015. (VII. 13.) kormányrendelet meghatározza a biztonsági eseménykezelő központok feladatait, illetve külön kiemeli, meghatározza a Kormányzati Eseménykezelő Központ feladatait.

Ennek megfelelően a GovCERT-en kívül Magyarországon a Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja, a Katonai CERT, valamint a kormányzati szektoron kívül két, önkéntes alapon működő CSIRT: a Hun-CERT és a NIIFI-CSIRT is működik.

4.4.1. A Kormányzati Eseménykezelő Központ

A Kormányzati Eseménykezelő Központ (GovCERT) a magyar kormányzat információmegosztó és incidenskezelő szervezete, amelyet az Ibtv. hozott létre.

A Kormányzati Eseménykezelő Központ 2015. október 1-óta a Nemzeti Kibervédelmi Intézet részeként látja el feladatait az állami és önkormányzati szerveknél. A Nemzeti Kibervédelmi Intézet három területre, szervezeti egységre osztható: a Nemzeti Elektronikus Információbiztonsági Hatóságra, a Kormányzati Eseménykezelő Központra, valamint a sérülékenységvizsgáló és biztonságirányítási területre. A korábbi széttagolt szervezeti modellhez képest most az Intézet keretein belül egyesült minden olyan tudás és képesség, amelynek köszönhetően megvalósulhat az állami intézmények hatékonyabb védelme, a teljes kormányzati IT-biztonsági életciklusban való együttműködés által.

Mivel jelen tananyag az eseménykezelő központok feladatait és működését tárgyalja, ezért a Nemzeti Kibervédelmi Intézet feladatai közül most csak a Kormányzati Eseménykezelő Központ feladatait tekintjük át. Ennek feladatait az Ibtv. és a 185/2015-ös kormányrendelet határozza meg. Ezek alapján a GovCERT az alábbi feladatokat látja el:

- 7/24 órában elérhető ügyeleti szolgálatot tart fenn, mely folyamatosan fogadja a rendszereket ért incidensek bejelentéseit, és megteszi az alapvető intézkedéseket.
- Biztonsági eseménykezelést végez az Ibtv. ügyfelei számára.
- Sérülékenységvizsgálat.
- Fenyegetésmenedzsment.

- Elemzés/értékelés.
- Részt vesz a nemzetközi és hazai kibervédelmi gyakorlatokban (például az ENISA által 2 évente megszervezett *Cyber Europe* gyakorlatban vagy a CSIRT-közösségek által szervezett gyakorlatokban).
- Képzést tarthat, részt vehet a tudatosító, valamint szemléletformáló kampányokban, szakértői-oktatói tevékenységet végezhet. Ennek keretén belül például a GovCERT – a Nemzeti Kibervédelmi Intézet részeként – minden év októberében részt vesz az ENISA által koordinált Európai Kiberbiztonsági Hónap (ECSM) tudatosító kampányában.
- Támogatja az elektronikus információs rendszer biztonságáért felelős személy kijelölését, valamint együttműködik vele.
- Riasztásokat ad ki a nemzetközileg publikált sérülékenységekről, jelentős hálózatbiztonsági eseményekről, és tájékoztatás küld a tudomására jutott sérülékenységekről.
- Figyelmeztetést ad ki a biztonsági eseményekre vagy fenyegetésekre utaló tevékenységekről az elektronikus hírközlési szolgáltató, az eseménykezelő központok, valamint a felhasználók számára.
- Jelentéseket és elemzéseket készít a magyar és nemzetközi irányokról, negyedévente jelentést készít a Tanács részére, valamint évente a központot irányító miniszter számára.
- Részt vesz az infokommunikációs biztonságra vonatkozó stratégiák és szabályok kidolgozásában.

A Kormányzati Eseménykezelő Központ nemzeti szinten együttműködik az eseménykezelő központokkal, a rendvédelmi szervekkel, a Katonai Nemzetbiztonsági Szolgálattal, a Nemzeti Média- és Hírközlési Hatóságon belül működtetett Országos Informatikai és Hírközlési Főügyelettel, az elektronikus hírközlési szolgáltatókkal, az elektronikus kereskedelmi szolgáltatókkal és az iparági szereplőkkel.

A nemzetközi együttműködésben a Kormányzati Eseménykezelő Központ úgynevezett *kapcsolattartó pontnak* nevezhető, hiszen a kormányrendeletben foglaltak szerint feladata a kapcsolattartás a nemzetközi hálózatbiztonsági szervekkel is. Ahhoz, hogy kapcsolattartó pontként a magyarországi eseménykezelő központok érdekeit is képviselni tudja a nemzetközi térben, elengedhetetlen a hatékony együttműködés, a folyamatos kommunikáció a Magyarországon működő többi CSIRT-tel.

Ennek megfelelően a GovCERT képviseli Magyarországot a NIS-irányelv által létrehozott CSIRT-ek hálózatában, Az ENISA felé ellátja a kapcsolattartó szerepkört, tagsággal rendelkezik a Forum of Incident Response and Security Teams (FIRST) CSIRT-közösségben, a Trusted Introducer (TI) CSIRT-közösségben, valamint együttműködik a Regionális Közép-Európai Kiberbiztonsági Platformmal és az IWWN nemzetközi CSIRT közösséggel is.

4.4.2. Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja

A Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (a továbbiakban: LRLIBEK) az Országos Katasztrófavédelmi Főigazgatóság keretein belül működik. Feladata a nemzeti létfontosságú rendszerelemeknél és létesítményeknél – az állam és az önkormányzatok által üzemeltetett rendszerek kivételével – a hálózatbiztonsági hatósági és eseménykezelési feladatok ellátása.

Incidenskezelési feladatait az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének szabályairól szóló 185/2015 kormányrendelet alapján látja el.

A kormányrendelet által előírt szabályoknak megfelelően az alábbi feladatokat látja el:

- ajánlások kiadása,
- nyilvántartás vezetése az incidensekről,

- tudatosítás, szakértők oktatása,
- együttműködési fórum működtetése,
- éves jelentés a szervezetet felügyelő miniszter számára.

4.4.3. A honvédelmi ágazat CERT-je: a Military CERT (MilCERT)

A honvédelmi célú elektronikus információs rendszerek esetében a honvédelmi ágazati elektronikus információbiztonsági eseménykezelő központ (MILCERT) látja el az Ibtv. szerinti CSIRT-feladatokat, illetve a katonai honvédelmi szervezetek felé történő kapcsolattartást.

4.4.4. A Hun-CERT

A Hun-CERT célja a magyar internetes társadalom segítése. A Hun-CERT az Internet Szolgáltatók Tanácsának (ISZT) támogatásával jött létre, a Magyar Tudományos Akadémia Számítástechnikai és Automatizálási Kutatóintézetében (MTA SZTAKI). Feladata az ISZT tagjainál felmerülő hálózat- és információbiztonsági incidensek esetében az incidenskezelés, az elemzés és a felderítés, az ügyfelei számára releváns esetekben különböző riasztások megosztása (például a GovCERT-től vagy a SANS Intézettől kapott riasztások), ezenfelül az ISZT-tagok és a teljes internetes társadalom tudatosságának növelése, hasznos információk, anyagok, tájékoztatók honlapjukon történő megosztása útján.

A Hun-CERT alapokmányában foglaltak szerint kapcsolatot tart egyéb CSIRT-ekkel, nemzeti és nemzetközi szinten.

4.4.5. NIIF-CSIRT

A NIIF-CSIRT a Nemzeti Információs Infrastruktúra Fejlesztési (NIIF) Intézet incidenskezelési csoportja. Az intézet a felsőoktatás, a kutatás és a közgyűjtemények közösségének (a továbbiakban: NIIF-tagintézmények) támogatására, segítésére jött létre. A NIIF-CSIRT feladata az incidenskezelés, az incidenskoordináció, a biztonsággal kapcsolatos információk továbbítása (tájékoztatás) a NIIF-tagintézmények számára.

A NIIF-CSIRT együttműködik a Kormányzati Eseménykezelő Központtal, valamint a GovCERT-tel.

4.5. Nemzetközi együttműködés

Az idők folyamán egyre kifinomultabb és kiterjedtebb incidenseket figyelhetünk meg, melyekre a CSIRT-ek körében izolált, koordinálatlan, esetleges, sőt akár eltérő válaszok, megoldások születtek.

Gyorsan egyértelművé vált a szakemberek számára: ahhoz, hogy egy kiterjedtebb incidensre gyors, hatékony és megfelelő választ lehessen találni, a CSIRT-ek együttműködésére van szükség. Az együttműködést viszont nehezítette az eltérő nyelvhasználat, az időeltolódás, az incidenskezelési eljárások és szabályok különbözősége, a különböző szabványok használata, valamint hogy a CSIRT-ek nem ismerték egymást.

Ezért a CSIRT-ek közötti együttműködés legegyszerűbb módja a kétoldalú, bilaterális együttműködések kialakítása, amely létrejöhet egy incidens vagy egy nagyobb projekt kapcsán, de a tapasztalatok alapján ez nem mindig elegendő egy nagyobb, kiterjedtebb incidens kezelése esetében.

A fent említett nehézségek áthidalása érdekében jöttek létre a CSIRT-együttműködések és CSIRT-közösségek. Közülük az első, a FIRST 1990-ben alakult meg. Azóta számos egyéb CSIRT-közösséget

hoztak létre a világon. Vannak nemzeti szintű együttműködések (CSIRT-ek és egyéb szervezetek együttműködése érdekében), regionális alapon szerveződött és szektorális együttműködést kialakító közösségek is.

A CSIRT-közösségek tagjai megosztják egymással a bevált gyakorlataikat, megvitatják a főbb sérülékenységeket, tájékoztatják egymást a főbb incidensekről, megvitatják szolgáltatásaikat, valamint együttműködnek egy határon átnyúló, több tagot is érintő incidens esetén. Egyes CSIRT-közösségek úgynevezett *kiberbiztonsági gyakorlatokat* is tartanak, amelyek során a közösségen belüli együttműködést és a szabályok betartását tesztelik és gyakorolják a tagállamok, példaincidensek imitálásával.

Kiemelendő, hogy a szakemberek az együttműködések során idővel azt is felismerték: nem feltétlenül elég a különböző CSIRT-ek együttműködése egy-egy incidens esetén, így mára már olyan együttműködéseket, közösségeket is működtetünk – nemzeti és nemzetközi szinten egyaránt –, amelyben a CERT-eken kívül az információbiztonsági hatóság, a rendőrség és esetleg a jogalkotó is részt vesz.

4.5.1. Az együttműködések jogi formája, szabályai

A sokféle együttműködés egyik különlegessége, hogy különböző jogi alapokon jöttek létre. Mindegyik együttműködés elengedhetetlen alapja a bizalom kiépülése, de ez akár évekig is tarthat.

Fontos kiemelni, hogy a közösségekben való együttműködés általában önkéntes alapú: a tagság és közösségen belüli szabályok jogi kötelezettséget általában nem szabnak a tagokra.

Számos esetben (főként a bilaterális együttműködések esetén) informális együttműködés figyelhető meg. Ha mégis szükség van az együttműködés formalizálására, például egy pénzügyi támogatás bevonása miatt, akkor erre különböző jogi megoldásokat találhatunk. Az egyik ilyen a *titoktartási megállapodás,* amely biztosítja, hogy a felek az együttműködés részleteit nem osztják meg más szervezetekkel. A másik lehetőség az úgynevezett *egyetértési megállapodás vagy szándéknyilatkozat* (Memorandum of Understanding, MoU), amely tulajdonképpen magában foglalja az együttműködés szándékát, valamint azonosítja az együttműködés pontos célját.

A *szerződés* a fenti együttműködési formáknál konkrétabb, formalizáltabb és részletesebb formáját valósítja meg az együttműködésnek.

A feladat meghatározása (Terms of reference) vagy az alapszabály (Charter) tekinthető a legalaposabb és részletesebb jogi dokumentumnak, mert magában foglalja az együttműködés célját, vízióját, pontosan nevesíti az összes résztvevőt, azok feladatait és felelősségét, a rendelkezésre álló forrásokat, a pénzügyi támogatásokat, az eljárásrendet és a határidőket is.

A 2016 augusztusában elfogadott Európai hálózat- és információbiztonsági irányelv tulajdonképpen elsőként teremtette meg egy CSIRT-közösség kötelező jogszabályi alapjait, feladatait.

4.5.2. A közösségek tagsági szabályai

A közösségek különböző módon kezelik a tagsági feltételeket, kérdéseket: néhányuk minden érdeklődő számára nyitott, és különösebb feltétel és felvételi eljárás nélkül csatlakozni lehet hozzájuk. Az ilyenek esetében előfordul, hogy a tagok számára *magatartási kódexet* (Code of Practice) fogalmaznak meg, de ennél komolyabb tagsági feltételeket és szabályokat nem szoktak előírni.

Van olyan közösség, amelyhez bárki csatlakozhat, ha a közösség által megszabott régióban vagy szakterületen fejti ki tevékenységét (például a regionális vagy szektorális közösségek esetében).

A fentieknél szigorúbb feltételt fogalmaznak meg azok a közösségek, ahol az új tagok felvétele a már tagsággal rendelkező szervezetek ajánlásához van kötve (ilyen például a FIRST).

A tagsági szabályok egyes közösségeknél előre szabályozott, többlépcsős akkreditációt írnak elő a CSIRT-ek számára.

Végül pedig ma már létezik olyan CSIRT-közösség is, amelybe az adott országok hivatalos úton jelölik ki az őket képviselő, a szabályoknak megfelelő CSIRT-et (ilyen közösség a CSIRT-ek hálózata).

Kiemelendő, hogy egyes CSIRT-közösségekben a tagság éves tagsági díjjal is jár.

A tagsági szabályokat a konkrét közösségeknél részletesebben ismertjük.

4.5.3. Nemzetközi közösségek

4.5.3.1. Forum of Incident Response and Security Teams (FIRST)

Ahogy ezt már fentebb említettük, a FIRST közösség volt az első CSIRT-együttműködést elősegítő közösség, ami 1990-ben jött létre, és ekkor még csak 5 taggal rendelkezett. Ez azóta minden évben bővül, különböző területekről, beleértve a kormányzati, katonai, piaci vagy az egyetemi CERT-eket is. Mára már 369 taggal rendelkezik a közösség, 79 különböző országból. Magyarországról a FIRST-nek a GovCERT a tagja, már 2006 óta.

A közösség célja, hogy segítse a tagjai közötti együttműködést a megelőzésben és az incidenskezelésben.

A közösség missziója alapján a tagok megosztják egymással a tapasztalataikat, jó gyakorlataikat, technikai információkat. A FIRST-tagok a közös tudásuk, eszközeik és tapasztalatuk által igyekeznek megteremteni egy biztonságos, globális elektronikus környezetet. A FIRST mára már saját szolgáltatásokkal is gazdagítja a CSIRT-közösség együttműködését és a CSIRT-ek egyéni képességeit.

A közösség a szabályok és működésének biztosítása érdekében létrehozott egy igazgatótanácsot és titkárságot, valamint rendelkezik két bizottsággal, amelyek az éves konferencia szervezéséért, valamint a tagsági kérdésekért felelősek.

4.5.3.2. Internet Watch and Warning Network (IWWN)

Az IWWN 2004-ben jött létre, azzal a céllal, hogy felgyorsítsa és elősegítse a nemzetközi együttműködést a kibertámadások kivédése és a sérülékenységek megszüntetése terén. A szervezet a közösséghez csatlakozott CSIRT-ek és hatóságok együttműködését hivatott biztosítani, összesen 15 országból: Amerikai Egyesült Államok, Egyesült Királyság, Japán, Kanada, Ausztrália, Franciaország, Finnország, Németország, Olaszország, Magyarország, Hollandia, Új-Zéland, Norvégia, Svédország, Svájc.

Ennek a közösségnek a tevékenysége nem nyilvános, így pontos feladatairól, működéséről és tagjairól sem tudunk átfogó, hiteles összefoglalást kapni.

4.5.3.3. Európai közösségek

A *Trusted Introducer*t (a továbbiakban TI) 2000-ben hozta létre az európai CSIRT-közösség, annak érdekében, hogy feltérképezzék a közös igényeket, valamint egy olyan szolgáltatási infrastruktúrát hozzanak létre, amely kulcsfontosságú támogatást nyújt az eseménykezelő központok számára.

Az együttműködésen és tapasztalat megosztáson túl a TI szolgáltatásokat nyújt a tagjainak, nyilvántartja az eseménykezelő csoportokat, valamint akkreditálja és tanúsítja a CSIRT-eket az érettségi szintjüktől függően.

Ennek megfelelően a TI-közösségen belül az eseménykezelő központok lehetnek *nyilvántartott, akkreditált vagy tanúsított* státuszban.

- Nyilvántartott tag: ha egy CSIRT csatlakozni szeretne a TI-közösséghez, akkor jelentkeznie kell, hogy vegyék nyilvántartásba. A jelentkezésének elfogadásához a TI-közösség tagjainak

támogatására van szüksége (legalább 2 CSIRT-től). A nyilvántartott csoportok adatai bekerülnek az elérhető nyilvántartásba, ezáltal részt vehetnek a TI-közösség rendezvényein. A nyilvántartott csoportoknak nincs tagsági díjuk.

- Akkreditált tag: csak nyilvántartott tagok jelentkezhetnek rá. Az akkreditáció eléréséhez a CSIRT-eknek egy úgynevezett meghívócsomagot kell teljesíteniük. A csomagban foglalt adatokat, dokumentumokat, nyilatkozatokat az akkreditációt igénylő CSIRT-nek 3 hónap alatt kell megküldenie a TI-hez. Az akkreditált tagok minden TI-szolgáltatáshoz automatikus hozzáférést kapnak.
- Tanúsított tag: csak olyan nyilvántartott tagok jelentkezhetnek rá, amelyek az akkreditációs eljáráson teljesen megfeleltek, valamint legalább egy TI-ülésen részt vettek. A tagoknak éves tagdíjat kell fizetniük. A tanúsítás megszerzéséhez az úgynevezett SIM3-model (Security Incident Management Maturity Model) segítségével 4 kategóriában (és 45 paraméterben) kell bizonyítaniuk érettségüket. A tanúsítás arra szolgál, hogy nemzetközileg elfogadott kritériumok alapján elismerje a CSIRT képességeit.

A *European Governnment CERTs Group,* azaz európai kormányzati CERT-ek csoportja az európai országok kormányzati CERT-jeinek informális társulása. A cél a tapasztalatok megosztása, együttműködés a határon átnyúló incidensek kezelésében, a szervezeti tapasztalatok, valamint a kutatásfejlesztés terén.

A szervezet a küldetésnyilatkozatában kiemeli, hogy egy nemzetközi környezet részét képezik, a tagok nagy része tagja a FIRST- és a TFCSIRT-közösségeknek is, valamint támogatják az ENISA törekvéseit, munkáját. Ezeket tiszteletben tartva működnek együtt ebben az informális társulásban, anélkül, hogy további szabályokat, eljárásrendeket hoznának létre.

A közösségnek 12 ország: Ausztria, Belgium, Dánia, Finnország, Franciaország, Norvégia, Németország, Hollandia, Svájc, Spanyolország, Svédország, valamint az Egyesült Királyság CSIRT-je és az EU-CERT a tagja.

A 2004-ben létrehozott európai uniós *Hálózat- és Információbiztonsági Ügynökség* (ENISA) egyik fő feladata tagállamok CSIRT-képességeinek növelése, támogatása, valamint az 526/2013/EU számú ENISA-rendelet 31. bekezdése alapján a CERT-ek és CSIRT-ek közötti önkéntes együttműködés, az információk és a bevált gyakorlatok cseréjének elősegítése, támogatása.

Ennek megfelelően az ENISA 2005 óta minden évben megtartja a tagállamok nemzeti és kormányzati CSIRT-jeinek az együttműködésére és információcseréjére szolgáló, *CERT-ek Európában* című workshopot. Ez az EU-s tagállamok nemzeti és kormányzati CSIRT-jei által alkotott közösség együttműködését biztosító fórum, munkacsoport. Azért kapta a workshop elnevezést, mert a többi közösségtől eltérően nincsenek eljárási szabályok, tagsági követelmények vagy kötelezettségek, a részt vevők mindössze minden évben megosztják egymással a főbb fejlesztéseiket, a feltárt sérülékenységeiket és azok megoldási javaslatait. A 2016 augusztusában elfogadott Európai hálózat- és információbiztonsági irányelv (NIS-irányelv) ezt az együttműködést formalizálva hozta létre az EU-s tagállamok CSIRT-jeinek közösségét, a CSIRT-ek hálózatát.

2012. szeptember 11-én az Európai Unió létre hozta a *CERT-EU*-t, az uniós szervezetek és intézmények védelme érdekében. A CERT-EU-ban dolgozó szakértők a főbb EU-s intézmények (Európai Bizottság, Európai Unió Tanácsa, Régiók Bizottsága stb.) IT-szakembereiből állt össze. A szervezet együttműködik a tagállamok CSIRT-jeivel és számos IT-biztonsággal foglalkozó céggel, főbb tevékenységei a megelőzés, a felderítés, a reagálás, a helyreállítás, valamint az információmegosztás.

2016. július 19-én jelent meg az Európai Unió hivatalos lapjában a hálózati és információs rendszerek biztonságáról szóló irányelv, amelynek kiemelt célja, hogy létrehozza az európai együttműködést, illetve hogy a létező önkéntes együttműködéseket formalizálja, ezért létrehozta az együttműködési csoportot, valamint *a CSIRT-ek együttműködését biztosító CSIRT-ek hálózatát.*

A CSIRT-ek hálózatának tagjai a tagállamok CSIRT-jei és az EU-CERT. Az ENISA támogatja a hálózat munkáját és a CSIRT-ek együttműködését, valamint ellátja a hálózat titkársági feladatait. Az Európai Bizottság megfigyelőként vehet részt munkában.

A CSIRT-ek hálózatának 2017. február 9-ig kellett megkezdenie a működést. Ennek megfelelően 2017. február 22-én és 23-án, Máltán került sor az első ülésére, amelynek során a tagok kidolgozták és elfogadták a hálózat eljárásrendjét (ez tartalmazza többek között az elnökség, a döntéshozatal, az ülések összehívásának szabályait, a szolgáltatási eszközök használatának rendjét, a tagállamok által delegálható tagok számát), valamint munkaprogramját.

A CSIRT-ek hálózatának feladatai az irányelv 12. cikke alapján a következők:

- A CSIRT-ek szolgáltatásainak és operatív képességeinek megosztása egymás között.
- Az egyes biztonsági eseményekre vonatkozó, nem bizalmas információk megosztása.
- Segítségnyújtás az érintett tagállamoknak határokon átnyúló biztonsági esemény estén.
- A hálózaton belüli operatív együttműködési formáinak (korai előrejelzés, kölcsönös segítségnyújtás, határon átnyúló incidens esetén az incidensre reagálás koordinációjának módja) megvitatása, megtervezése. Erre vonatkozóan iránymutatást is készít.
- A hálózat- és információbiztonsági gyakorlatok eredményének és tanulságainak értékelése.
- A tagállam CSIRT-jének kérése esetén a tagállam joghatósága alatt történt esemény és az arra adható koordinált válaszlehetőségek megvitatása.
- A hatóságok együttműködését biztosító együttműködési csoport tájékoztatása a munkájáról.

4.5.3.4. Regionális együttműködések

A *Közép-európai Kiberbiztonsági Platform* (Central European Cyber Security Platform, a továbbiakban CECSP) 2013-ban jött létre Ausztria és Csehország kezdeményezésére. Tagjai kormányzati, nemzeti és katonai CSIRT-ek, nemzeti biztonsági hatóságok, valamint minisztériumok képviselői Magyarországról, Csehországból, Ausztriából, Lengyelországból és Szlovákiából.

A platform létrehozásának a célja, hogy a kibertámadások elleni védekezés során regionális együttműködésben hatékonyabb védekező- és ellenállóképességre tegyenek szert a résztvevő országok. Kiemelendő, hogy az országok közötti történelmi kötelékeken túl hasonló fejlettségi szint és érdeklődési irány figyelhető meg az információbiztonsági szervezetek között. Ennek köszönhetően hasonló kihívásokkal, problémákkal kell nap mint nap szembe nézniük.

A többi CSIRT-együttműködéshez hasonlóan itt is az a cél, hogy a tagjok megosszák egymással a tapasztalataikat, beszámoljanak a jelentősebb sikeres és sikertelen támadásokról, gyakorlatok által növeljék képességeiket és az együttműködést a tagok között, valamint közösen munkálkodjanak a kutatás-fejlesztési projektek terén.

Fontos célja a platformnak, hogy a tagállamok a nemzetközi környezetben egy már előre harmonizált, közös álláspontot képviseljenek, ezzel már jelentős véleménytöbbséget alkotva a nagyobb nemzetközi közösségekben (például EU, NATO és OSCE). Ezért a tagok munkaprogramot fogalmaztak meg a platform számára.

4.5.3.5. Information Sharing and Analysis Centers

A kibertámadásokra és sérülékenységekre való gyors reagálás érdekében a CSIRT-közösségeken túl létrejöttek úgynevezett információmegosztó és elemzőközpontok (Information Sharing and Analysis Centers, a továbbiakban ISAC) vagy más néven információmegosztó és elemző szervezetek (Information Sharing and Analysis Organisations) is. Ezek tulajdonképpen a köz- és magánszféra közötti együttműködést segítik elő szektoronként.

A CSIRT-ek és CSIRT-közösségek mellett azért volt szükség az ISAC-ok létrehozására, mert az ilyen szervezetek lehetőséget nyújtanak arra, hogy egy adott szektor összes szereplője a szabályozótól, a szolgáltatón át a szektorhoz tartozó CSIRT-ig közösen dolgozhassanak a problémák és kihívások megoldásán, legyen az jogszabályi, technikai, esetleg egy incidensből adódó kérdés.

Kiemelendő, hogy minden szektornak megvannak a maga technikai, jogi és egyéb sajátosságai, valamint a jellemző támadási és incidenstrendjei. Az ISAC-ok lehetővé teszik, hogy ezeket a kérdéseket az adott területen jártas, hasonló problémával rendelkező szakemberek vitassák meg.

Az ISAC tagjai a többi közösségekhez hasonlóan megosztják tapasztalataikat, elemzéseiket, segítik egymást, évente 2-8 alkalommal üléseket tartanak, attól függően, hogy a szektor képviselői szerint mennyi találkozó hasznos és szükséges az együttműködés hatékonyságához.

Minden ISAC különálló és egyedi: saját szabályokkal, eljárásrenddel, céllal és különböző tagokkal rendelkezik. A titkársági funkciókat mindig valamelyik tag látja el.

Alapvetően az információmegosztó és elemzőközpontokban tag lehet a szektorért felelős CSIRT, a szektorhoz tartozó szolgáltató vagy cég képviselője, a kormányzat részéről pedig a nemzeti CSIRT, a szektor szabályozásáért felelős kormányzati szerv (általában minisztérium), valamint a kiberbűnüldöző hatóság képviselője.

Az ISAC-ban a tagsági feltételeket minden esetben az ISAC saját maga, illetve tagjai szabályozzák. Léteznek ISAC-ok nemzetközi, európai, valamint nemzeti szinten egyaránt.

Hollandiában a kikötők, a repterek, a pénzügyi szervezetek, a vízügy, az ivóvíz-ellátás, a telekommunikáció, az egészségügy, a biztosítások, a kormányzat, a nyugdíjrendszer, a nukleáris energia és a multinacionális vállalatok területén működnek nemzeti szintű ISAC-ok.

Európai szinten eddig még csak két információmegosztó és elemzőközpont jött létre: az energiaszektorban a European Energy – Information Sharing Analysis Centre (EE-ISAC) valamint a pénzügyi szektorban az European Financial Institutes – Information Sharing and Analysis Centre (FI-ISAC).

Napjainkban számos ISAC működik nemzetközi szinten is, például az 1999-ben létrejött, pénzügyi szolgáltatók Innformációmegosztó és elemzőközpontja (FS-ISAC) világszerte az összes banki és pénzügyi szolgáltatást nyújtó szervezetet szívesen látja a tagjai között.

2008-ban jött létre az európai pénzügyi szektor információmegosztó és elemzőközpont (European Financial Institutes – Information Sharing and Analysis Centre, FI-ISAC). Tagjai a nemzeti vagy kormányzati CSIRT-ek, a bűnüldöző hatóságok, valamint a szektor képviselői, továbbá részt vesz a központ munkájában az ENISA, az EUROPOL, az Európai Bizottság, az Európai Központi Bank, valamint az Európai Fizetési Tanács is.

A központ célja, hogy a tagok információt osszanak meg incidenseikről, esettanulmányokat, sérülékenységeket tegyenek közzé, technológiai trendeket és támadásokat vitassanak meg, valamint együttműködjenek a bankszektort érintő bűncselekmények esetében.

Az európai pénzügyi szektor információmegosztó és elemzőközpontjának (European Energy – Information Sharing Analysis Centre, EE-ISAC) létrejöttét 2015 novemberében jelentették be a European Utility Week eseményen. A kormányzati és piaci szereplőkön túl a központ munkájában részt vehetnek a szolgálatók, az akadémiák és nonprofit szervezetek is.

Az EE-ISAC-ot európai uniós kutatás-fejlesztési támogatásból, az úgynevezett DENSEK-projekt keretében hozták létre, jelenleg 19 tagja van, amelyeknek célja – a többi együttműködéshez hasonlóan – az információmegosztás, a sérülékenységek, incidensek megvitatása, a bevált gyakorlatok megosztása.

4.6. CSIRT létrehozása

A fentiek alapján látható, hogy egyre több eseménykezelő központ létrehozására van szükség napjainkban. A jogszabályi előírások vagy az egyes területeken növekvő incidensek, sérülékenységek száma miatt időről időre megfogalmazódik a szervezetek, szektorok vagy kisebb csoportok körében,

hogy szükség van egy eseménykezelő központra egy adott szervezeten vagy ágazaton belül. Ekkor felmerül a kérdés, hogy hogyan kell CSIRT-et létrehozni, milyen jó gyakorlatok, tapasztalatok vannak ezen a területen, milyen szabályoknak kell megfelelni stb.

Számos szervezet létezik, amely igény esetén tanácsot ad, segít a CSIRT létrehozásában. A CERT/CC, az ENISA, valamint a TI egyaránt készített a létrehozásról szóló útmutatót vagy kézikönyvet, valamint segítséget lehet tőlük kérni a CSIRT létrehozására vagy fejlesztésére. Hollandiában a Nemzeti Kibervédelmi Központ szintén nyújt ilyen tanácsadó szolgáltatást.

A CERT/CC 1998-ban elsőként hozta létre a CSIRT-eknek szóló kézikönyvét, melyben a CSIRT fogalmát, szolgáltatásait, illetve a létrehozásakor megfontolandó kérdéseket, a szükséges lépéseket fogalmazza meg. A kézikönyvet 2003-ban frissíttettékaz aktuális trendek és fejlődés alapján.

Az Európai Hálózat- és Információbiztonsági Ügynökség feladata, hogy támogassa és segítse az Európai Unió tagállamait a megfelelő IT-biztonsági politikájuk, szervezeteik létrehozása és fejlesztése során. Ennek keretében a tagállam kérésére támogatja a CSIRT-ek létrehozását, fejlesztését egyaránt. 2006-ban az ENISA készített egy tanulmányt, *Részletes leírás a CSIRT-csoportok létrehozásáról*[8] címmel.

A holland kormányzati CERT (GOVCERT.NL) publikálta a *CERT-in-a-box* című esettanulmányt, mely átfogó leírást ad a GOVCERT.NL és a holland nemzeti riasztási szolgálat (De Waarschuwingsdienst) létrehozása során szerzett tapasztalatokról, illetve a CSIRT-ekre vonatkozó főbb információkról (típusok, feladat, működés stb.). Ezenkívül a nagyobb CSIRT-közösségek (például TI, FIRST) is közzétettek a honlapjukon összefoglalókat, ismertetőket a CSIRT létrehozásáról.

A CERT létrehozásáról és fejlesztéséről szóló anyagok és esettanulmányok összességében ugyanazokat a fő lépéseket, javaslatokat fogalmazzák meg, csak eltérő megközelítést alkalmaznak, illetve a szükséges intézkedéseket más csoportosításban vagy sorrendben fogalmazzák meg.

Az ENISA, a Trusted Introducer (TI) és a CERT/CC ajánlásai alapján az alábbi lépéseket, feladatokat kell elvégezni, megfontolni egy CSIRT létrehozása során, de fontos megjegyezni, hogy ezek egy része történhet egyszerre vagy a leírtaktól eltérő sorrendben is.

1. A CSIRT lényegének áttekintése

A CSIRT létrehozásához kapcsolódó feladatok megkezdése előtt a szakirodalom javasolja a CSIRT fogalmának, típusainak, működésének és feladatainak alapos áttanulmányozását. Ez a lépés elengedhetetlen ahhoz, hogy el tudjuk dönteni, pontosan milyen CSIRT-et szeretnénk létrehozni.

2. Az ügyfélkör azonosítása és elemzése

Pontosan meg kell tudni határozni, hogy ki lesz a CSIRT ügyfélköre, kiknek fog szolgáltatásokat nyújtani. A leendő ügyfelekkel fel kell venni a kapcsolatot, és felmérni, hogy pontosan milyen szolgáltatásokra van szükségük, milyen IT-biztonsági fenyegetések vagy incidensek fordultak elő ebben a körben, mely kommunikációs csatornák alkalmazását találják a legmegfelelőbbnek az információk átadására.

Az ügyfélkör igényeinek felmérésére különböző módszereket ajánl a szakirodalom. A két legelterjedtebb módszer a SWOT-analízis, amelynek során az erősségeket, a gyengeségeket, a lehetőségeket és a veszélyeket azonosítják, valamint a PEST-analízis, amely a CSIRT működési környezetének politikai, gazdasági, társadalmi és technológiai körülményeit segít felmérni.

A CSIRT-ek különböző kommunikációs csatornákat használhatnak:

- weboldal,
- az ügyfelek számára fenntartott zárt felhasználói felület a weboldalon,

[8] *Részletes leírás a CSIRT-csoportok létrehozásáról.* Elérhető: www.enisa.europa.eu/publications/csirt-setting-up-guide-in-hungarian/at_download/fullReport (a letöltés ideje: 2017. április 20.)

- az incidens bejelentéshez használandó webes űrlapok,
- levelezőlista,
- papír alapú levelek,
- rendszeres (havi/ éves/negyedéves) jelentések,
- személyes e-mail,
- telefon,
- fax.

A fenti kommunikációs csatornák közül nem feltétlenül szükséges az összes alkalmazása; meg kell találni azokat, amik a leginkább alkalmasak arra, hogy a CSIRT leendő ügyfélkörének minél nagyobb részéhez eljusson a szükséges információ. Egyes útmutatók még a PGP használatára is felhívják a figyelmet a biztonságos kommunikáció biztosítása érdekében.

3. Szolgáltatások kiválasztása

Mivel már felmérték a leendő ügyfelek elképzeléseit, igényeit, illetve az ügyfelek körében tapasztalt trendeket, ez segíthet a szükséges szolgáltatások kiválasztásában.

Kezdetben az úgynevezett alapvető szolgáltatásokkal kell megkezdeni CSIRT tevékenységét, tehát az incidenskezelést és -elemzés, a bejelentéseket, valamint a riasztások kiadását kell biztosítani.

Az alapvetőkön túl lehetnek olyan szolgáltatások, melyekre az ügyfélkör igényei alapján szükség van, de kifejlesztésére csak a CSIRT elindítását követően kerül sor, így ezeket a hosszú távú célok között kell feltüntetni.

4. Küldetésnyilatkozat

A vevőkör igényeinek azonosítását és a szolgáltatások kiválasztását követően a *küldetésnyilatkozat vagy vízió* megfogalmazása a következő fontos lépés.

A küldetésnyilatkozat megfogalmazásához elengedhetetlen, hogy a CSIRT-et pontosan definiáljuk a létrehozandó CSIRT-re vonatkozó elképzelések és a szakirodalom által nyújtott kereteken belül.

A küldetésnyilatkozat rövid, tömör és lényegre törő, az idő múlásával is megfelelően tudja képviselni a szervezet elképzeléseit és létrejöttének, működésének célját, a CSIRT alapfunkcióját, általános célját fogalmazza meg.

A szakirodalom javasolja, hogy a CSIRT vízióját, küldetésnyilatkozatát kommunikáljuk az érintett felek (felsővezetés és a leendő ügyfelek) felé. A tőlük kapott visszajelzések segíthetnek a CSIRT létrehozásának további fázisaiban, az információbiztonsági szabályzat megfogalmazásában.

5. Üzleti terv létrehozása

Az üzleti terv magában foglalhatja a pénzügyi terv megfogalmazását, a CSIRT elhelyezésének szabályait, valamint a szervezet belső struktúrájának kialakítását, a kiválasztott szolgáltatások kifejlesztését, megteremtését.

Mindenképp fontos a tervezés során (akár az üzleti terv kidolgozása során vagy azt megelőzően) az adott országban érvényes CSIRT-ekre és feladataikra vonatkozó szabályozás megismerése, hogy azt figyelembe véve, a jogszabályoknak megfelelően alakítsuk ki a szervezetünket. Magyarországon például a 185/2015-ös számú kormányrendelet tartalmazza az alapvető információkat és szabályokat a CSIRT-ekről.

A következő feladat a pénzügyi modell kidolgozása, amihez meg kell határozni, hogy pontosan mire (eszközök, munkatársak) van szükség a kiválasztott szolgáltatások működtetéséhez. Ezt alapvetően a szolgáltatás minősége, valamint a CSIRT által alkalmazni szükséges munkatársak száma határozza meg.

Az egyik legfontosabb kérdés e tekintetben, hogy az incidenskezelési szolgáltatásra és a technikai támogatásra az ügyfeleknek heti hét napon keresztül 24 órában szükségük van vagy pedig főként hivatali időben veszik igénybe őket.

A költséghatékonyabb megoldás szerint a CSIRT csak a hivatali időben nyújtja a megelőző és válaszintézkedési szolgáltatásait, azon túl pedig telefonos elérhetőséget biztosít a jelentős incidensek bekövetkezésének esetére. Ezen modell alkalmazása során jelentősen kevesebb munkatárs alkalmazása is elég a CSIRT megfelelő működéséhez.

Egyes esetekben van arra mód, hogy a CSIRT pénzt kérjen – tagsági díj formájában – a szolgálgatásaiért. Ez a megoldás ritkán alkalmazható (főként az üzleti világban), így a költségvetés tervezésénél nem igazán lehet ezzel a bevételi lehetőséggel számolni.

6. A szervezeti modell kialakítása

Nagyon fontos eldönteni, hogy hogyan épüljön fel a szervezet. Abban az esetben, ha a CSIRT egy adott szervezeten belül jön létre, akkor a szervezeti modellt az anyaszervezet és az ott alkalmazott szabályok és szokások fogják eldönteni.

Minden esetben szükség van egy vezetőre (vezérigazgatóra), valamint egy úgynevezett üzemeltetési műszaki csoportra. Ennek a csoportnak van egy szakmai vezetője (csoport- vagy osztályvezető), és a szolgáltatásokat nyújtó technikai munkatársak, valamint a kutatók alkotják még a csoport részét.

Akkor van szükség a legtöbb munkatársra, ha a CSIRT független, tehát nem más szervezet része, mert ilyenkor szükség van a irodavezetőre, személyügyekkel foglalkozó munkatársra, valamint kommunikációs és jogi tanácsadóra is.

Abban az esetben, ha a CSIRT-et egy meglévő szervezeten vagy több CSIRT-csoportot magába foglaló közösségen, hálózaton belül helyezik el, akkor a szervezet működésének biztosításáért felelős munkatársak (jogi, kommunikációs, HR) feladatait az anyaszervezeten belüli munkatársak el tudják látni.

A személyügyekért felelős munkatárs felvétele és bevonása a CSIRT létrehozásának folyamatába nagy fontosságú lehet, hogy a segítségével időben tudják definiálni a munkatársaktól elvárt kompetenciákat (szakmait és személyit egyaránt).

Az ENISA által késztett tanulmány szerint egy CSIRT-nek minimum 4 teljes munkaidős technikai munkatársra van szüksége. Ez esetben hivatali időben mindössze két feladatot tud ellátni a CSIRT: az egyik az incidenskezelés, a másik pedig a tanácsadás és a riasztások kiküldése.

7. A CSIRT elhelyezése, az iroda használata

Számos, az irodára vonatkozó fizikai biztonsági szabály, követelmény létezik, amelyek a beléptető rendszer használatára, a CSIRT irodáinak és bejáratának kamerás megfigyelésére, a biztonságos információtechnológiai eszközök használatára, a redundáns internetkapcsolat biztosítására, valamint a zárható lemezszekrényekre, a széfek elhelyezésére, a bizalmas információk és anyagok tárolására vonatkozó szabályokat, kritériumokat fogalmazzák meg.

Az új CSIRT-eknek a nemzeti szabályokat kell figyelembe venni, míg a nem független CSIRT-ek esetében az anyaszervezet szabályai is kötelező erejűnek tekintendők.

Egyes útmutatók ide sorolják a szolgáltatások nyújtásához és a CSIRT működésének alapszintű körülményeihez szükséges eszközök beszerzésének és biztonságos telepítésének elvégzését is.

8. Információbiztonsági szabályzat használata

Minden CSIRT-nek el kell készítenie a saját információbiztonsági szabályzatát, amely magában foglalja az üzemeltetési és adminisztratív eljárások, folyamatok leírását.

A szabályzatnak az alábbi szabályokat kell tartalmaznia:

- beérkező információk osztályozása,
- információk kezelésének szabályai,
- információközlés, -megosztás szabályai (például az incidensekre vonatkozó adatok),
- az adatkommunikáció és az e-mail-forgalom védelmi titkosításának lehetősége, szabályai.

A szabályzatban foglaltaknak meg kell felelniük a nemzeti és az EU-s jogszabályoknak, illetve a különböző nemzetközi megállapodásokban rögzített szabályoknak egyaránt. A nemzeti jogszabályok előírhatják az eredetileg nem kötelezően betartandó szabványok betartását is.

A figyelembe veendő szabályozások (nemzeti és nemzetközi szinten egyaránt):

- infokommunikációra és telekommunikációra vonatkozó szabályozások,
- információbiztonságra vonatkozó szabályozások,
- elektronikus aláírásról szóló szabályozások,
- adatvédelmi szabályok,
- pénzügyi és számviteli szabályozások,
- társasági jogról szóló jogszabályok,
- informatikai bűnözésről szóló szabályozások.

A szakirodalom az ISO-szabványok, valamint a nemzeti szabványok (például British Standards BS7799 vagy a francia EBIOS) figyelembevételét javasolja.

9. Együttműködés

A CSIRT megfelelő működése és jól informáltsága (a bevált gyakorlatok megismerése, hogy a fontos sérülékenységi, fertőzési információkról mielőbb értesüljenek) érdekében fontos, hogy együttműködést alakítson ki más CSIRT-ekkel, csatlakozzon a CSIRT-közösségek munkájához.

Erre általában már a CSIRT létrehozásának korai szakaszában sor szokott kerülni, hiszen a CSIRT-közösségek tagjai szívesen osztják meg tapasztalataikat, látják el tanácsokkal az újonnan létrejövő CSIRT-et.

Mindenképp javasolt az adott országban működő CSIRT-ek közötti együttműködéshez csatlakozni, kétoldalú együttműködést kialakítani az adott CSIRT tevékenységéhez köthető, egyéb szektorális vagy hasonló ügyfélkörrel rendelkező CSIRT-tel.

Javasolt a különböző nemzetközi CSIRT-együttműködések (szektorális, regionális, európai vagy bármely nagy globális nemzetközi közösség) között is megtalálni az új CSIRT számára legmegfelelőbbeket.

Ahogy a korábbi fejezetekben szó volt róla, a legtöbb közösség nyitott, belépési kritériumokat, tagdíjat nem ír elő tagjainak. Első körben javasolt az ilyen közösségekhez csatlakozni.

10. A folyamatok menetének, az üzemeltetési és technikai eljárásoknak a kialakítása

Ezen folyamat során kerül sor a már kiválasztott szolgáltatások munkafolyamatainak részletes leírására, meghatározására.

Ide sorolandó az incidenskezelés részletes szabályozása, az incidens bejelentéséhez használatos adatlap kialakítása, a figyelmeztetések és bejelentések menetének és szabályainak (az információk

értékelésének és kockázatfelmérésének menete, módszere, az információk terjesztési szabályainak és menetének) kidolgozása, meghatározása.

11. A CSIRT munkatársainak oktatása

A kézikönyvek és tanulmányok javasolják, hogy a CSIRT-be felvett műszaki, technikus szakemberek vegyenek részt CSIRT-képzéseken a feladataik alaposabb elsajátítása és megismerése érdekében. Ma már több szervezet vagy intézmény is nyújt ilyen képzéseket.

Az ENISA 2008 óta ad ki képzési anyagokat, illetve tart különböző képzéseket IT-biztonsági szakemberek számára. Az ENISA-képzéseken az Európai Unió tagállamainak CSIRT-jei vehetnek részt. Arra is van lehetőség, hogy a tagállamok nemzeti és kormányzati CSIRT-jei felkérjék az ENISA-t, hogy tartson képzést helyszínen a CSIRT teljes állományának.

Az ENISA mára számos képzési anyagot állított össze, amelyek alapvetően 4 fő területre terjednek ki: CSIRT létrehozása, operatív feladatok, technikai feladatok, valamint a jogi és együttműködési területekre.

A TRANSITS egy olyan európai projekt, amelynek célja az új CSIRT-ek létrehozásának és a már működő CSIRT-ek bővítésének, fejlesztésének támogatása speciális tanfolyamok által. A TARANIS keretében szervezett képzések során a munkatársak a CSIRT-szolgáltatások nyújtásához kapcsolódó főbb jogi, szervezeti, üzemeltetési kérdésekkel foglalkoznak, oktatási műhelyt szerveznek és műhelymunka segítségével igyekeznek gyakorlati tudást biztosítani a résztvevőknek.

A CERT/CC főként menedzsereknek és műszaki munkatársaknak szóló képzéseket tart a CSIRT-ek létrehozásáról és irányításáról, az incidenskezelésről, valamint az incidenselemzésről.

12. Gyakorlás és a CSIRT hivatalos bejelentése

A CSIRT előkészítése, kidolgozása, a munkatársak felvétele és képzése után már csak a CSIRT létrejöttének hivatalos bejelentése hiányzik. A hivatalos bejelentést a vezetésnek, az ügyfeleknek, a CSIRT-közösségeknek, illetve az anyaszervezetnek (abban az esetben, ha van) kell címezni. Gyakran nyílt nap vagy nyitóünnepség szervezésével biztosítják, hogy emlékezetes és ünnepélyes legyen a CSIRT létrejöttére vonatkozó bejelentés.

Egyes szakirodalmak azt javasolják, hogy a hivatalos működés és bejelentés előtt hasznos, ha a CSIRT egy szűk ügyfélkör bevonásával egy rövid tesztidőszakot, gyakorlást tart. Ennek folyamán az éles indulás előtt le lehet ellenőrizni a kialakított szolgáltatásokat, a folyamatokat, valamint a műszaki munkatársak tudását.

13. A CSIRT hatékonyságának növelése

Az ügyfelek és partnerek visszajelzései, valamint a nyilvántartási adatok (bejelentett incidensesek száma, az incidensekre adott válaszok ideje, sikeresen lezárt és elhárított incidensek, preventív, megelőző szolgálgatások hatékonysága, népszerűsége) alapján meg kell vizsgálni a CSIRT működésének hatékonyságát.

Az adatok alapján azonosítani lehet, hogy mely területen van szükség további fejlesztésekre, módosításokra, illetve hogy milyen további szolgáltatás létrehozására lehet szükség.

A TI által készített útmutató kiemeli, hogy egy CSIRT létrehozása és működtetése hosszú folyamat: a létrehozás körülbelül 12-18 hónap, míg az ügyfelek bizalmának és elismerésének elnyerése várhatóan további 12-18 hónap lehet.

Felhasznált irodalom

Részletes leírás a CSIRT-csoportok létrehozásáról. Európai Hálózat- és Információbiztonsági Ügynökség, 2006. Elérhető: www.enisa.europa.eu/publications/csirt-setting-up-guide-in-hungarian/at_download/fullReport (a letöltés ideje: 2017. április 5.)

Handbook for CSIRTs (2003). Elérhető: http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf (a letöltés ideje: 2017. április 1.)

Incident Handling Management. Európai Hálózat- és Információbiztonsági Ügynökség, 2016. Elérhető: www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/setting-up-a-csirt#Incident_Handling_Management (a letöltés ideje: 2017. április 5.)

CERT Cooperation and its further relevant facilitation by relevant stakeholders. Európai Hálózat- és Információbiztonsági Ügynökség, 2006. Elérhető: www.enisa.europa.eu/publications/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders (a letöltés ideje: 2017. április 30.)

CSIRT Capabilities. Guidelines for national and governmental CSIRTs. Európai Hálózat- és Információbiztonsági Ügynökség, 2015. Elérhető: www.enisa.europa.eu/publications/csirt-capabilities (a letöltés ideje: 2017. április 15.)

Horváth Gergely Krisztián (2014): *Incidens-menedzsment, BCP, DRP integráció. A biztonság eseménykezelés, és illeszkedése a működésfolytonosság tervezéshez, és az informatikai szolgáltatásfolytonosság tervezéshez.* Budapest, NKE, ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel. Elérhető: http://vtki.uni-nke.hu/uploads/media_items/incidens-menedzsment_-bcp_-drp-integracio.original.pdf (a letöltés ideje: 2017. április 6.)

Pokladnik, Mason (2007): *An Incident Handling Process for Small and Medium Businesses.* SANS Institute. Elérhető: www.sans.org/reading-room/whitepapers/incident/incident-handling-process-smallmedium-businesses-1791 (a letöltés ideje: 2017. április 20.)

Killcrece, Georgia (2005): *Incident management white paper.* CERT Coordination Center. Elérhető: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=295919 (a letöltés ideje: 2017. április 4.)

5. BIZTONSÁGI MŰVELETI KÖZPONTOK (SOC-K)

Dr. Hámornik Balázs Péter – Orbók Ákos

5.1. Bevezető

A kiberbiztonság területén az utóbbi időben a figyelem fókuszába egy specializált műveleti célú szervezeti egység került: a biztonsági műveleti központ vagy ismertebb angol rövidítése szerint a SOC (Security Operations Center). A szervezetek és a szervezeti egységek olyan kihívásokkal nézne szembe napjainkban, mint az általános szaktudás és az emberi erőforrások hiánya a szektorban annak következtében, hogy nagymértékben megnőtt az igény a kiberbiztonsági szakemberekre. Ez nehézséget gördít a SOC-k kialakítása elé. Ennek okán a klasszikus tankönyvi, 3 vonalból álló SOC megvalósítása gyakran nem lehetséges, hanem szolgáltató partnerek bevonásával kell a megoldást megtalálni. Elöljáróban fontos kiemelni, hogy a jó SOC nem csupán egy riasztásfeldolgozó műveletsor, hanem fenyegetettségekkel kapcsolatos hírszerzési (Threat Intelligence, TI) adatok felhasználója és előállítója, amely szoros kapcsolatban dolgozik az incidenskezelést ellátó csapattal (hacsak ez nem a SOC része is egyben), illetve proaktívan keresi a lehetséges fenyegetettségeket (hunting). A SOC nemcsak saját, szervezeten belüli formában valósítható meg, hanem kiszervezetten, szolgáltatók által is. Az ilyen szolgáltatókkal különböző hibrid modellek alakíthatók ki a SOC bizonyos részeinek, funkcióinak házon belül tartására, illetve kiszervezésére. Jellemző az első vonalbeli riasztáskezelés és a TI partnerek általi biztosítása.

Minden SOC számra elsődleges kihívás a rálátás megteremtése és biztosítása a védeni kívánt informatikai rendszerre. Mielőtt bármely szervezet is belevágna egy SOC kialakításába, lényeges, hogy fenntartható költségvetést tervezzen be az üzemeltetése első két-három évére. Ennyi időre mindenképp szükség van a csapat, a folyamatok és a technológia kialakulására, megszilárdulására. Ennél hamarabb elvárni a befektetések megtérülését idejekorán véget vethet az SOC életének.

Ugyan a külső biztonsági szolgáltatóknak való kiszervezés egyre gyakoribb, és a fenti területeken kétségkívül gyümölcsöző is, viszont az újonnan elterjedt, analitikán alapuló felhasználói és entitásviselkedés-elemző módszerek (User and Entity Behavior Analytics, UEBA) kiszervezése nem javasolt. Ilyen eszközökkel sikerrel lehet a belső fenyegetettségeket elhárítani, amikor a szervezet valójában a rossz szándékú saját alkalmazottai ellen védekezik. Ehhez elengedhetetlen a saját üzleti működés és a dolgozók rutintevékenységeinek ismerete, mivel az UEBA a normálistól való eltérés detektálásával működik.

A legjellemzőbb trendek az SOC-ok fejlődésében, amiket példáula Gartner piackutató is jósol a közeljövőre:

- A proaktív fenyegetettség, a vadászat (hunting) elterjedése.
- Eltávolodás a kizárólag riasztásokra épülő működési modelltől, mivel a túl sok riasztás kezelése a hatékonyságot akadályozza (ehelyett a fent említett proaktív szemlélet kerülhet előtérbe).
- Az automatizálás és az eszközök összehangolása egyre nagyobb hangsúlyt kap.
- Megjelennek álcázásos technikák a támadók szándékának és eszközeinek jobb megértésre.
- Nemcsak a fenyegetettséggel kapcsolatos hírszerzés használata (TI), hanem az ilyen információk előállítása és megosztása is elterjed.
- Egyre nagyobb arányban fognak a szervezetek használni fejlett analitikai eljárásokat, különösen UEBA-eszközöket.

- A SOC hatékonyságának értékelésre különböző éles helyzeteket modellező gyakorlatok alkalmazása is jellemző lesz.

5.2. A biztonsági műveleti központok fogalma és modelljei

A biztonsági műveleti központ vagy SOC (Security Operations Center) egy olyan csapatot jelent, amely éjjel-nappali műszakban működik, és amelynek egyaránt feladata a megelőzés, a felderítés és a kiberbiztonsági fenyegetésekre, eseményekre adható válaszok kidolgozása, valamint a szervezet vagy létesítmény biztonsági előírásainak vizsgálata és értékelése (Muniz–McIntyre–AlFardan 2015)Operating, and Maintaining Your SOC The complete, practical guide to planning, building, and operating an effective Security Operations Center (SOC.

Amellett, hogy egy szervezet a saját maga védelmére létrehoz egy SOC-ot, üzletileg sok esetben előnyösebb, ha más, erre szakosodott szolgáltatóktól veszi igénybe a biztonsági műveleti központok nyújtotta állandó védelmet. Ezt a szolgáltatást „Managed SOC”-nak nevezik, és a szolgáltatást egy „Managed Security Service Provider” (MSSP) szervezet nyújtja. A menedzselt szolgáltatás egy megosztott erőforrásokból felépülő szolgáltatás, amely nemcsak egyetlen szervezetre vagy személyre épül. Az SOC ilyenkor földrajzi elhelyezkedésében elkülönül a védelme alá tartozó szervezettől, akár külön kontinensen is lehetnek. Egy MSSP és annak SOC-csapatai egyszerre több szervezetet is kiszolgálnak különböző kibervédelmi szolgáltatásokkal (például a SOC mellett forensics vagy malware analízis).

Egy teljesen működőképes SOC állandó üzemet igényel, legalább 8-10 fővel. Csak a fenntartáshoz két ember szükséges műszakonként, akik párosával, 12 órás váltott műszakokban dolgoznak 3 vagy 4 napot, egyenlő arányú pihenőnapokkal. Ez egy kétfős műszak esetén lehetővé teszi, hogy egy fő monitorozással, míg a másik a kivizsgálásokkal foglalkozzon, valamint jól megoldott a helyettesítés (például egy betegség esetén) is (Muniz et al. 2015)Operating, and Maintaining Your SOC The complete, practical guide to planning, building, and operating an effective Security Operations Center (SOC. Azonban ez nem tartalmazza a vezetési, a fluktuációs, a szabadságokkal kapcsolatos problémákat, illetve olyan más speciális funkciókat, mint a rosszindulatú programok visszafejtése, a kriminalisztika és a fenyegetettségek proaktív elemzése (Threat Intelligence, TI) és kezelése, amelyek nem minden SOC központi tevékenységi körébe tartoznak bele.

Alapvetően öt SOC-ot különböztethetünk meg működési modelljük alapján. Ezeket az 1. táblázatban foglaltuk össze.

1. táblázat

Az SOC működési modelljei

SOC-modell	Jellemzők	Jellemző alkalmazása
Virtuális SOC	Nincs saját külön létesítménye. Részmunkaidős csapattagok. Reaktív működés: kritikus riasztás, incidens esetén kezd működni. Ez az elsődleges modell, ha teljesen kiszervezik az MSSP-nek a SOC-t.	Kis- és közepes vállalkozások, kisebb nagyvállalatok.
Többfunkciós SOC/ NOC	Külön létesítmény és kijelölt csapat, amely nemcsak a biztonságot érintő feladatokat lát el, hanem más kritikus IT-műveleteket is végez egy helyen, a nap 24 órájában, ezzel csökkentve a költségeket.	Kis- közepes és alacsony kockázatú nagyvállalatok, ahol a hálózati és biztonsági funkciókat már ugyanezek vagy átfedő személyek és csoportok végzik.
Elosztott vagy társmenedzselt SOC	Saját és félig erre kijelölt csapattagok. Tipikusan heti 5 napban, napi 8 órás üzemelés (8/5). Az MSSP bevonásakor ez társmenedzselt.	Kis- és közepes méretű vállalatok.

SOC-modell	Jellemzők	Jellemző alkalmazása
Saját SOC	Saját, elkülönült létesítmény. Külön csapat. Teljesen házon belüli működés. 24/7-es működés.	Nagyvállalatok, szolgáltatók, nagy kockázatú szervezetek.
Irányító SOC	Más SOC-k koordinálása. Threat Intelligence szolgáltatás, helyzettudatosság és további szakértelmek nyújtása a SOC-knak. Ritkán vesz részt közvetlenül a napi működésben.	Óriásvállalatok és szolgáltatók; kormányok, hadsereg, hírszerzés.

Forrás: BARROS–CHUVAKIN 2016

5.3. A működéshez lényeges képességek, szakértelem – és a szakemberek megtartása

A SOC elemzői munkakörnek általában alacsony a munkaerő-megtartó képessége: még azok a szolgáltatók is, amelyek karriert és fejlődési lehetőséget is képesek nyújtani, állandóan küzdenek a SOC-elemzők három-négy évnél hosszabb megtartásával. Ennek okai között megjelenik a váltott műszakokban végzett és monoton munka. Emellett a terület egy ritka és keresett készségkészletet igényel, és ez azt eredményezi, hogy gyakran az ugródeszka szerepét tölti be a munkavállalók karrierjében, tovább súlyosbítva azt a globális képzett szakemberhiányt, amely az ágazatban tapasztalható.

Egy létszámhiányos vagy tapasztalatlan elemzőkből álló SOC azért fog küzdeni, hogy a funkcióit ellássa. Így az események észlelése és a fenyegetésekre való reagálás hatásfoka alacsony lesz. Ha a szervezet hosszabb ideig nem rendelkezik kellő személyzettel, ez szintén hozzájárulhat az elemzők lemorzsolódásához, és a meglévő szakemberekre nagyobb munkaterhelés kerül.

Ezek alapján azt lehet megállapítani, hogy a SOC-ban a kezdetektől ki kell alakítani egy stratégiát a munkaerő megtartására, mert a biztonsági ipar ezen a részén hiány alakult ki – és marad fent várhatóan a következő években is – a képzett biztonsági elemzőkben. Ez az SOC tervezése és üzemeltetése során is a humán erőforrással foglalkozó szakemberek bevonását indikálja.

Amennyiben a finanszírozás korlátozottan biztosított, a döntéseinknél fent kell tartani az egyensúlyt az üzleti érdekek és a kritikus belső biztonsági funkciók között. Bizonyos alacsonyabb szintű biztonsági funkciókat, mint az eszközkezelés (device management) végezheti egy MSSP, amely képes tartani a megfelelő szolgáltatási szintet, valamint kedvezőbb áron dolgozik, viszont előnyös, ha az elemzés és az incidenskezelés házon belül marad. Az MSSP-ek szintén képesek támogatást adni a belső SOC-csapatnak a váratlan vagy szokatlan események kezelésében, olyan időszakokban, mint a szabadságolások, a nagy biztonsági incidensek vagy a létesítményekkel kapcsolatos problémák esetén.

Ennek biztosítására a fejlesztés elején érdemes kijelölni jól meghatározott célokat és mutatókat, amik szükségesek ahhoz, hogy a SOC biztonsági céljai érvényesülni tudjanak az üzleti érdekekkel szemben.

A kezdetekkor anyagilag biztosítani kell az első két-három évben az SOC működését, valamint azt, hogy a költségvetés fenntartható legyen a továbbiakban is. Általában ennyi idő alatt a folyamatok és a technológia kezelése beágyazódik a szervezetbe, és a dolgozók megfelelő szintű jártasságot szereznek. Tehát a SOC egy hosszú kifutású fejlesztés, amelyben nem gyors a megtérülés, viszont a technológiai és emberi tényezők kikristályosodásával garantálható a legmagasabb szintű információbiztonság. Emellett fontos kiemelni, hogy a menedzselt szolgáltatásként működő SOC (managed-SOC, MSSP által) nem minden esetben optimális megoldás: javasolt a kritikus biztonsági funkciók házon belül tartása.

5.3.1. A biztonsági események és az információ kezelésének kritikus képességei

A biztonsági események sikeres kezeléséhez elsődlegesen naplókezelés (log management) és jelentéskészítés, dokumentálás szükséges, olyanok, amelyek megfelelnek a szektor szabályozásainak. Ahhoz, hogy a SOC a legfontosabb területeken helyt álljon, három helyzetre kell tervezni:

1. A szabályozásoknak való megfelelésre (Compliance).
2. Fenyegetettségmenedzsmentre (Threat Management).
3. Security Information and Event Management (SIEM) szoftverre, amelyet megfelelően üzemeltenek és konfigurálnak.

A következő kritikus képességek azonosíthatók az SOC hatékonyságában:

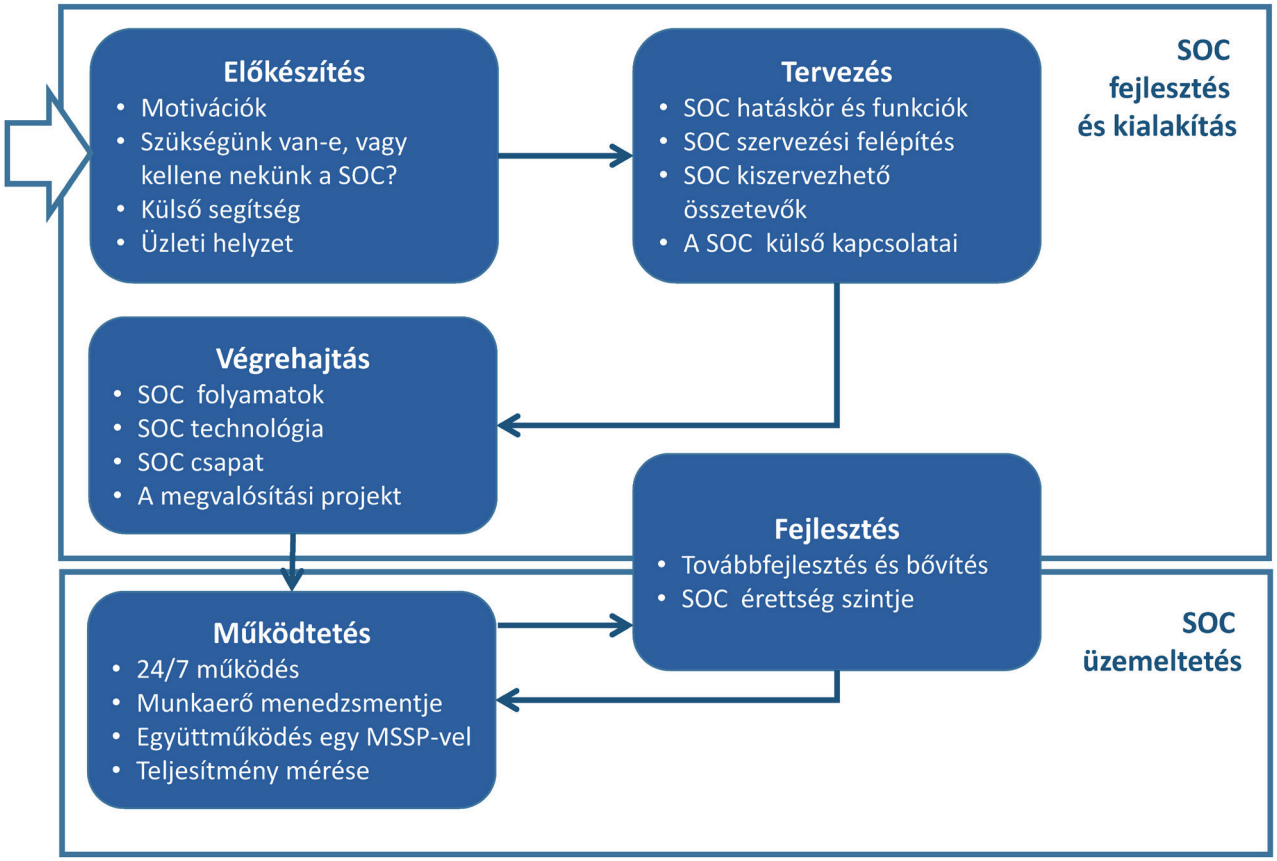
- Valós idejű monitorozás: a támadások lefolyásának nyomon követése és elemzése az összes alkalmazáson és a rendszeren keresztül, valamint a felhasználói tevékenység megfigyelése, nyomon követése és elemzése.
- Threat Intelligence (TI): a fenyegetések proaktív felderítése friss és aktuális adatok, az ismert támadási minták alapján.
- Viselkedésprofilozás: riasztással minden normális viselkedéstől való eltérés esetén a megfigyelés során.
- Adat- és felhasználói monitorozás: a privilegizált felhasználók tevékenységének és az érzékeny adatokhoz való hozzáférésük folyamatos monitorozása legtöbbször része a szabályozásoknak való megfelelésnek.
- Alkalmazás-felügyelet.
- Elemzés és analitika.
- A naplófájlok kezelése és jelentés (report) készítése.
- Az eszközök és alkalmazások telepítésének, illetve támogatásának egyszerűsítése.

Az SOC-ok középpontjában a fent említett SIEM-szoftverek állnak, amelyek összesítik, összekapcsolják a rendelkezésre álló biztonsági szempontból releváns adatokat, és riasztásokat adnak az események kockázatosnak ítélt mintázatai esetén. Ezekre a központi fontosságú szoftverekre a későbbiekben részletesen kitérünk.

5.3.2. A SOC tervezésének, megvalósításának, üzemeltetésének és fejlesztésének kulcskérdései

A legtöbb SOC központi képessége és feladata a biztonsági szempontból releváns események monitorozása. Általánosságban az SOC feladatkörei közé tartozik továbbá a fenyegetettségek és sebezhetőségek kezelése, a biztonsági eszközök kezelése és karbantartása, a kiberbiztonsági incidensek kezelése, a szabályozásoknak való megfelelés biztosítása, a biztonsági tréningek. Az információbiztonsági képzések biztosítása a szervezetben, illetve a szabályozásoknak való megfelelés biztosítása egyre kevésbé része napjainkban egy SOC feladatainak. Ezzel szemben a fenyegetettségek proaktív felderítése (Threat hunting) és a Threat Intelligence lassanként új SOC-funkciókká válnak.

A következőkben időrendben tekintjük át a SOC-ot érintő legfontosabb kérdéseket, a tervezéstől a létező biztonsági műveleti központ továbbfejlesztéséig.



1. ábra

Egy SOC fejlesztése, kialakítása és üzemeltetése

Forrás: BARROS–CHUVAKIN 2016

5.3.3. Előkészítés

A legjellemzőbb motiváció, ami egy SOC kialakítását indokolja, a kiberbiztonsági műveletek centralizálásának igénye, a szervezet egészére való rálátás javítása, a fenyegetettségek feltárásának javítása. Emellett az egyre növekvő, észlelt vagy valós kockázatok kezelésének igénye, a fenyegetettségeknek való kitettség csökkentése is lényeges motiváló tényező. Mindezek mellett jogszabályok és előírások is meghatározhatják a központosított kibervédelmi monitorozást és műveleteket, amire a SOC nyújtja a legjobb megoldást.

Az előkészítés fontos előfeltétele, hogy a szervezet alapvető IT-üzemeltetési érettséggel rendelkezzen. A monitorozáshoz naplózási folyamatok, a logok megfelelő generálása, kezelése, megtartása szükséges, és az a tudás a hálózati kontextusról, ami ezek értelmezését biztosítja. Emellett lényeges előfeltétel és a tervezés során figyelembe veendő, hogy a monitorozást és a biztonsági események detektálását végző SOC mellett incidenskezelésre, válaszadásra alkalmas csapatnak is kell a szervezet rendelkezésére állnia (bár ez esetenként tervezhető a SOC-on belülre is).

Egy szervezet a SOC megvalósításában és üzemeltetésében is tervezhet külső partnerekkel. E partnerek között lehet olyan, amelyik megépíti a SOC-ot, amelynek kiszervezhető a SOC (MSSP, managed SOC), amellyek megoldható a saját SOC-csapat kiegészítése külső szakemberekkel, állandó jelleggel vagy időszakosan (például súlyos incidensek idejére). Azt azonban figyelembe kell venni, hogy a felelősség nem szervezhető ki. A végső felelősség a biztonságért a szervezeté marad. A legjobb MSSP-partner sem tud incidenst detektálni olyan rendszerben, amire nincs rálátása vagy nincs hozzáférése.

5.3.4. Tervezés

A tervezés első lépése, hogy a fent említett SOC-tevékenységek és -felelősségek közül kiválasztják a megvalósítani kívánt elemeket (belső vagy kiszervezett formában). Az incidensekre valós válaszadás (Incident Response, IR) funkciójának SOC-on belül vagy kívül (külön Computer Security Incient Response Team-ben, azaz CSIRT-ben) való megvalósítása szerint a következő előnyök és hátrányok jelenhetnek meg.

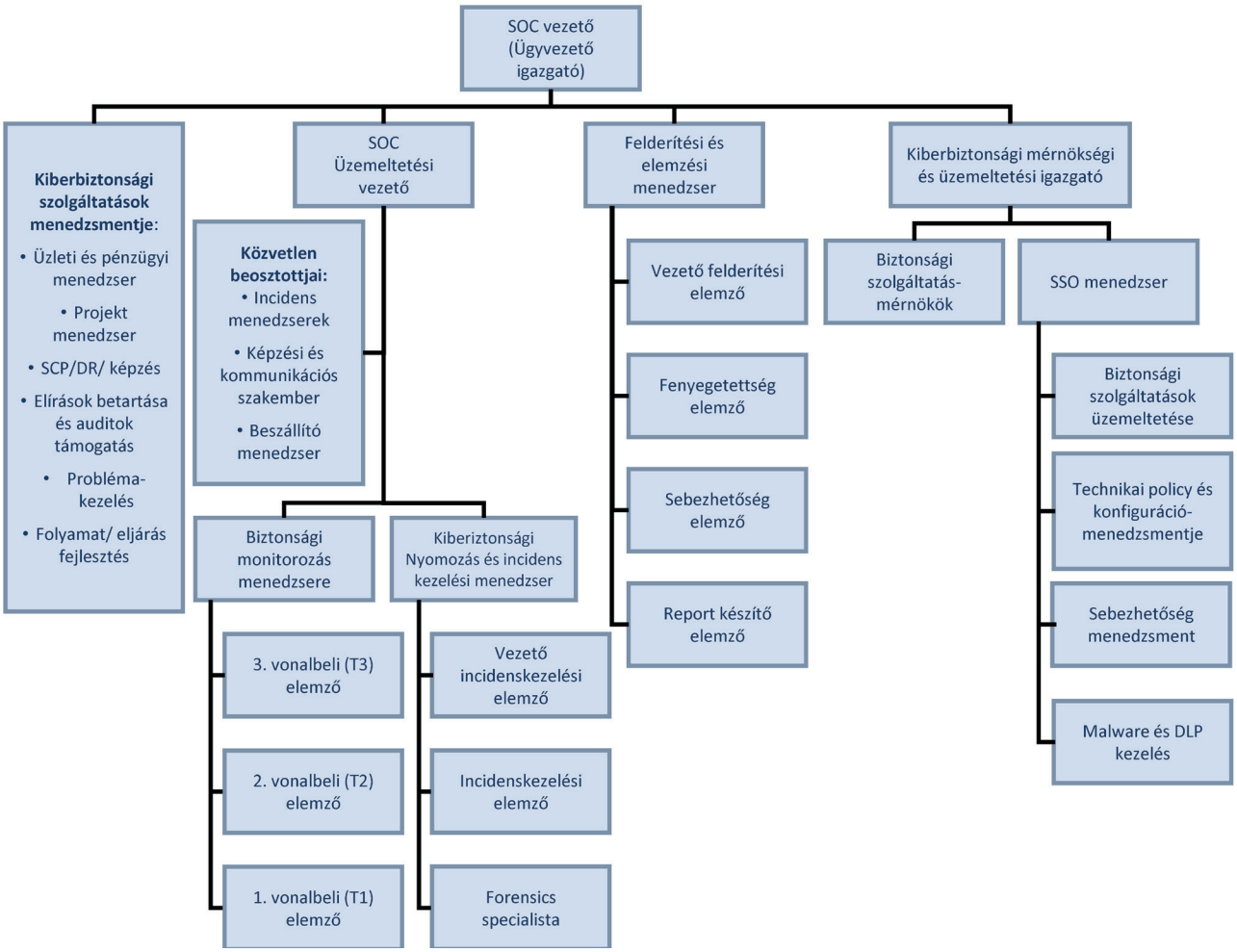
2. táblázat

Előnyök és hátrányok az IR külső vagy belső formája esetén

	Előnyök	Hátrányok
IR a SOC részeként	A felderítés és a reagálás közötti szorosabb integráció. Csökkenti az erőforrás-igényeket, mivel nem szükséges extra menedzsmentréteg. Több lehetőséget kínál a karrierfolyamathoz és a munkahelyi rotációhoz a SOC-on belül.	A feladatokat el kell különíteni, amikor a SOC személyzetével kapcsolatos figyelmeztető jelzések vizsgálata zajlik. Az IR-csapat függetlenségének hiánya a felderítéssel és a kezdeti riasztással kapcsolatos kérdésekre utal, amelyet a SOC kezel. Összetett a kiszervezése, mert az IR egy olyan funkció, amely nem könnyen szervezhető ki. A magasabb IR-munkaterhelés negatívan befolyásolhatja az észlelési tevékenységeket.
IR irányítása egy elkülönített CSIRT-tel	Az IR csapat függetlensége lehetővé teszi a SOC-forrásokkal kapcsolatos események kivizsgálását. Könnyebb kiszervezni a SOC felügyeleti funkciót, mivel az IR-tevékenységeket külön kezelik.	Valószínűleg párhuzamosságokat okoz és kiegészítő erőforrást igényel (legalább vezetési szinten). Csökkenti a karrierfejlődési lehetőséget a SOC-on belül. A kis jelentőségű SOC-szerepek valószínűleg kevésbé vonzóak a tehetségek vonzására.
IR a SOC és a CSIRT között elosztva	Csökkenti a CSIRT erőforrás-igényét, amikor teljesen különválasztják a csoportokat (a SOC lehet az IR-csapat technikai része). Javítja a CSIRT-ben bekövetkező események átadását a teljesen különálló csoportokhoz képest.	Nincsenek tisztázva a felelősségek és a szerepek. A függetlenség esetleges hiánya a SOC-forrásokkal kapcsolatos események kivizsgálása során.

Forrás: Barros–Chuvakin 2016

A SOC-ok megvalósításának öt, korábban bemutatott modellje terjedt el (lásd 1. ábra). Ezek közül a tervezés fázisában szükséges választani.



2. ábra

A saját SOC szervezeti felépítése

Forrás: MUNIZ et al. 2015

A külső partnereknek való kiszervezésre visszatérve fontos kiemelni, hogy az MSSP-k rendszerint biztonsági monitorozást vagy biztonsági eszközök kezelését ajánlják ügyfeleiknek. Kevéssé jellemző, hogy nem napi üzemeltetési jellegű feladatokat (például biztonsági vezetés, átfogó programok megtervezése) kiszerveznének. Emellett szintén nem jellemző az IT-rendszerfelügyeleti munkák ilyen jellegű kiszervezése, a teljes szervezeti IR és az UEBA (User and Entity Behaviour Analysis) külső partnereknek való átadása. Ezeket összegezve a következő kevert SOC-modellek lelhetők fel a piacon azok előnyeivel és hátrányaival (3. táblázat).

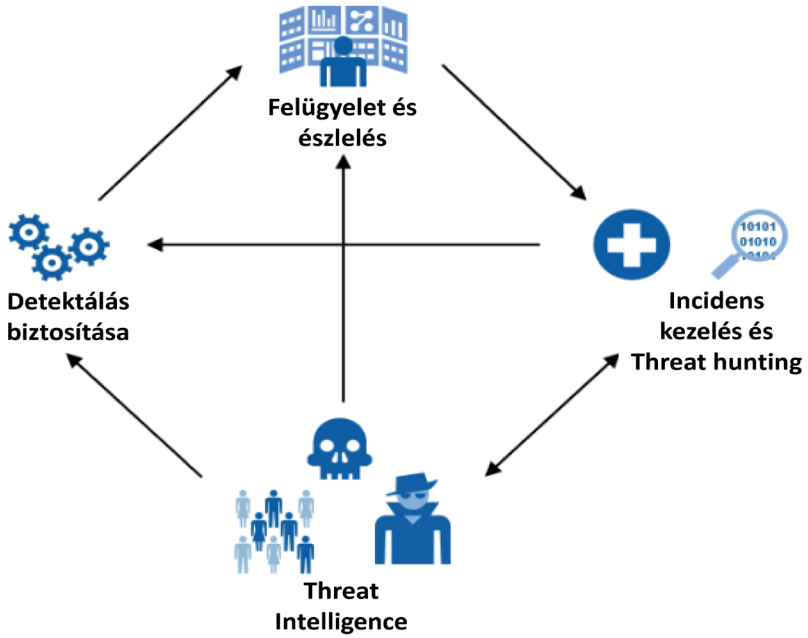
3. táblázat
Kevert SOC-modellek

Modell	Előnyök	Problémák	Részletek
MSSP mint 1. szintű elemző, 2. és 3. szint házon belül	A korlátozott belső csapathoz érkező riasztások csökkentett mennyisége. Képes arra, hogy beállítsa a figyelmeztető jelzéseket egy csapatnak. Csökkennek a személyzet irányításához kapcsolódó kiadások (nincs szükség a nagy fluktuáció kezelésére az 1. szinten).	Az MSSP a biztonsági figyelmeztetések egyetlen forrása, így magas fokú bizalomra van szükség a szolgáltató irányába. Csak a riasztásokban bíznak. Az első szinten nem lehet kinevelni a személyzetet.	A belső napló tárolása (például SIEM, naplókezelő eszközök vagy biztonsági adatréteg) szükséges ahhoz, hogy működjön.
MSSP felügyeli a kevésbé kockázatos, jellemzően belső rendszereket, egy belső SOC a kulcsrendszereket és alkalmazásokat	A termék szolgáltatója ellenőrzi a terméket érő támadásokat (MSSP), de a szervezeten belüli fenyegetések házon belül kezelhetők. Réteges védelem, anélkül, hogy egyedül az MSSP-re támaszkodnának a fenyegetés felderítése érdekében. Erősség alapú megközelítés.	Kihívások a hálózat nyilvános és magánterületét érintő behatolások nyomon követésével. Feltételez egy alkalmas belső SOC-ot.	Ideális esetben egy belső csapatnak hozzáférést kell kapnia minden naplóhoz: azoknak, akik egy MSSP-hez fordulnak és azoknak is, akik nem.
MSSP éjjel, belső SOC napközben	Állandó elérés magas személyi követelmények nélkül.	Az adatátadási eljárás kialakítása kihívást jelent. Az elemzők kereséseinek szinkronizálása szintén kihívás. Még mindig van valamilyen képesség arra, hogy reagáljon a nem szokványos órákban bekövetkezett eseményekre (igényre rendelkezésre álló személyzettel).	Ugyanaz, mint az előző esetnél, egy belső csapatnak hozzáférést kell kapnia minden naplóhoz: azoknak, akik egy MSSP-hez fordulnak és azoknak is, akik nem.
MSSP a kiválasztott feladatokhoz, minden más ellenőrzés a belső SOC-ban	Taktikai okokból átruházza azokat a feladatokat, amelyek jobbak és/vagy olcsóbbak lehetnek a külső kezeléshez, kivéve a belső személyzetet fontosabb feladatait.	Tartalmaz egy már kiépült, kiforrott belső SOC-ot. Az adatátadás és a közös munkafolyamat kialakítása nehéz lehet.	Az MSSP szerepe itt tanácsadói szerepkörré fejlődik, és jobban kezelhető egy tanácsadó cég által.

Forrás: Barros–Chuvakin 2016

5.3.5. A SOC megvalósítása

Ahogy azt megfogalmaztuk, a SOC fő tevékenysége *a monitorozás és a detektálás.* Napjainkban jellemzően egyre nagyobb hangsúly esik a fenyegetettségek proaktív megismerésére, az ezekkel kapcsolatos hírek, tapasztalatok megosztására, amit Threat Intelligence, TI néven említünk. A modern SOC-ok feladatai között így megjelenik a proaktív keresés (vadászat, threat hunting) és a Threat Intelligence is.



3. ábra

A SOC feladatai

Forrás: BARROS–CHUVAKIN 2016

A SOC megvalósítása során lényeges az eszköztár megválasztása. Az eszközök három csoportba sorolhatók: rálátást biztosítanak, elemzést tesznek lehetővé és cselekvést, menedzselést szolgálnak.

5.3.5.1. A rálátást, láthatóságot biztosító eszközök

- Endpoint Detection and Response (EDR): TI-forrásokból származó végpontokra vagy indikátorokra vonatkozó figyelmeztető jelzések vizsgálata. Threat hunting esetén is használják.
- NFT (Network Forensics Tools) és hálózati forgalmat elemző (Network Traffic Analysis,NTA) eszközök: a figyelmeztető jelzések vizsgálata és további összefüggések megszerzése a hálózatbeli gyanús tevékenységekkel kapcsolatban. Threat hunting eszközként is használják. Esetenként hálózati forgalomgyűjtő eszközök is használhatóak a teljes Layer 7 csomagrögzítő eszköz helyett; a netflow gyűjthető a SIEM-ben is.
- Sebezhetőséget értékelő eszközök (Vulnerability Assesment, VA): a meglévő biztonsági rések azonosítása a rendszerben. Sérülékenységek kezelésére használják vagy csak a nyomon követéshez és az eszközleltárhoz kapcsolódó további kontextuális információ gyűjtésére.

5.3.5.2. Elemző eszközök

- SIEM (Security Information and Event Management): a különböző technológiákból és forrásokból származó események és logok konszolidálására és korrelálására, figyelmeztetések generálására vagy a gyanús, illetve privilegizált tevékenységek elemzésére használják. Egyetlen keresőfelületet biztosít a naplófájlokhoz, illetve fel lehet használni vizsgálati és threat hunting tevékenységekre is. A SIEM-et gyakran tekintik az SOC legfontosabb eszközének.

- UEBA (User and Entity Behaviour Analysis eszköz): a felhasználók és más hálózati entitások gyanús viselkedéseinek azonosítására használják. A riasztások forrásaként vagy finomhangolásukra és gazdagítására, illetve a SIEM-információk kontextusának megértésére is használható.
- Malware elemzés és Sandboxing: a rosszindulatú szoftverek (vagy gyaníthatóan rosszindulatú szoftverek) hálózatban történő azonosítására használják. Cloud-sandbox-okhoz való hozzáférés is része lehet alkalmazásuknak.

5.3.5.3. Cselekvést és menedzsmentet lehetővé tevő eszközök

- SOAR (Security Operation, Analytics and Reporting): támogatják a munkafolyamat-kezelést, az automatizálást, az elemzéseket és a jelentéstételt. Ez lehetővé teszi a biztonsági műveleti csoportok számára, hogy automatizálják és rangsorolják a biztonsági operatív tevékenységeket, adatot szolgáltassanak, jelentést tegyenek, támogatva az üzleti döntéshozatalt. Három elsődleges SOAR technológiatípus létezik: a biztonsági incidensek megválaszolása, a biztonsági műveletek automatizálása, a fenyegetettség- és a sebezhetőségmenedzsment.
- Munkafolyamat- és esetkezelés (Workflow and Case Management): az SOC-tevékenységek menedzsment eszközeként használják, munkafolyamat-kezelést biztosít az automatizáláshoz és az SOC műveletek értékelését lehetővé tevő mutatókat ad. A munkafolyamatok és az automatizálási funkciók gyakran szerepelnek a SOAR-eszközökben is.
- Threat Initelligence Platforms (TIP): a TI felhalmozásának, konszolidációjának, pontosításának és megosztásának megkönnyítésére használható. Az SOC-t vagy egy másik, TI-fókuszú csapatot is támogathat.

Az eszközök ezen széles palettájából jellemzően hármat tartanak elengedhetetlennek (ezt nevezik SOC Nuclear Triad-nek is): a SIEM-et, az NFT-t és az EDR-t. A minimum, hogy egy SOC SIEM-et használ elemzésre és különböző sebezhetőségértékelő (VA) eszközöket a rálátás biztosítására, viszont idővel és az érettséggel egyre több eszköre jelenik meg igény. Ennek része az is, hogy számos eszköz integrálható a SOC-ban lévő rendszerekbe, hogy a heterogenitás és a túlzott komplexitás elkerülhető legyen. Az integrációk legjellemzőbb fókuszpontja a SIEM szokott lenni.

A SOC nemcsak technológiából, de szakemberek csapatából vagy együttműködő csapataiból is áll. A legfőbb tevékenységet jelentő monitorozást jellemzően legalább két vonalba (level vagy tier) szervezett elemző csapat látja el, egymáshoz eszkalációs sorrendben kapcsolódva:

- Az első vonal (Level/Tier 1): az itt szolgálatban lévő elemzők az első körös riasztásrendezést, áttekintést végzik. Ők az első pont, ahol a SOC belép egy eseménnyel kapcsolatos tevékenységbe. Jellemzően 24/7-es munkarendben dolgoznak, több műszakban váltva egymást.
- A második vonal (Level/Tier 2): itt nagyobb tapasztalatú és képzettebb elemzők dolgoznak, akik az első vonal által hozzájuk továbbított riasztásokat elemzik, és reagálnak azokra. Bizonyos esetekben ezek a szakemberek igény szerint dolgoznak, nem éjjel-nappalos műszakokban.

További fontos szerepek a SOC-csapatban a következők lehetnek: a SOC-csapatot vezető menedzser, a műszakot vezető menedzser, a SOC műszaki és tartalmi feladatait vezető menedzser, TI-elemző, IR-szakértő (amennyiben ez a SOC-on belül van).

A SOC csapattal kapcsolatos, a megvalósítás során leginkább lényeges kérdés a képzett szakemberek hiánya a területen. Tapasztalataink szerint nemcsak a nemzetközi, de a hazai piacon is jellemző az, hogy a SOC-szakemberek karrierútja az első vonalból indul (Level 1 SOC analyst), ahova fiatal pályakezdőket vesznek fel, és őket képzik, ezzel elkerülve a tapasztalt szakemberek költséges alkalmazását. Az ilyen karrierút-tervezés implikálja, hogy a következő vonal és a specifikusabb SOC-pozíciók felé haladni tapasztalattal, idővel, képzéssel lehet (szenioritás jellemzi ezeket a feladatköröket). Ez a megközelítés nem segít abban, hogy az első vonalban dolgozó elemzőket megtartsák,

elégedettségük és munkájuk minősége kellő szintű legyen. Viszont a képzésükbe invesztált költségek kárba vesznek, ha ők távoznak a szervezetből. Rájuk nehezedik a legnagyobb stressz is, pontosan az alacsony státuszú pozíció és a 24/7-es munkarend miatt, ami a kiégés és pályaelhagyás okozója lehet. A kockázatot fokozza az, hogy a munkaerőhiány miatt a cégek egymástól agresszívan igyekeznek szakembereket átcsábítani. E probléma kivédését szolgálhatja, ha a különböző SOC-vonalakat és -szerepeket nem szenioritás alapján értelmezzük, hanem a SOC célját szolgáló, azonosan fontos, de más képességeket igénylő területekként. Ezek között a szakemberek megadott rend szerint rotálhatók, ami a klasszikus munkapszichológia egyik alapvető elégedettségjavító módszere. Ezzel az elégedettség és a hatékonyság is növelhető, viszont a stresszes (például első vonalbeli) pozíciókban a kiégés csökkenthető. Az erősen versengő munkaerőpiaci helyzet miatt a szakemberek javadalmazásán és a motiváló karrierúton kockázatos megtakarítani.

Egy saját, fizikai SOC-biztonsággal üzemelő szint megvalósítása jellemzően 18-24 hónapot vesz igénybe. Ebben benne van a fizikai hely létrehozása (irodabérlés és annak berendezése a SOC igényei szerint), a szakemberek kiválasztása, felvétele, kiképzése a csapatba, az eszközök beszerzése és telepítése, végül az üzemeltetés folyamatainak kidolgozása és finomhangolása.

A megvalósítás összefoglaló jellegű mérföldkövei a következők.

1. Személyzet
   – Kiválasztás, felvétel vagy cégen belüli munkatársak átvétele.
   – A szerepek kijelölése.
   – Képzés és a képességbeli hiányok lefedése.
   – Megtervezni a külső partnerek szakembereinek esetleges bevonását.
2. Folyamatok
   – A fő folyamatok definiálása (például riasztásértékelés, -rendezés, eszkalálás stb.).
   – A meglévő IT-biztonsági folyamatok áttekintése és az SOC-hoz alakítása.
   – A folyamatok átadása azt azokat végrehajtó elemzőknek.
3. Eszközök
   – A meglévő eszköztár áttekintése.
   – A szükséges eszközök beszerzése.
   – Eszközök telepítése.
   – A tartalom létrehozása (például SIEM riasztási szabályai, use case-ek).
   – Integráció.
   – A folyamatok illesztése a meglévő eszközökhöz.

Ahogy az előző fázisokban, úgy a megalósítás során is fontos szerep juthat a külső partnereknek és tanácsadóknak:

- MSSP-által alkalmazott szakemberekkel időlegesen áthidalható az egyes szakterületek hiánya (azok felvételéig).
- A tanácsadó cégek szakembereinek alkalmazásával (akár évekre is) lehetőség nyílik speciális képességek eltanulására a csapatban, ami segíti a SOC érettségének kialakulását.
- A monitorozási esetek (use case-ek) egy kisebb része a partnerek segítségével valósítható meg.

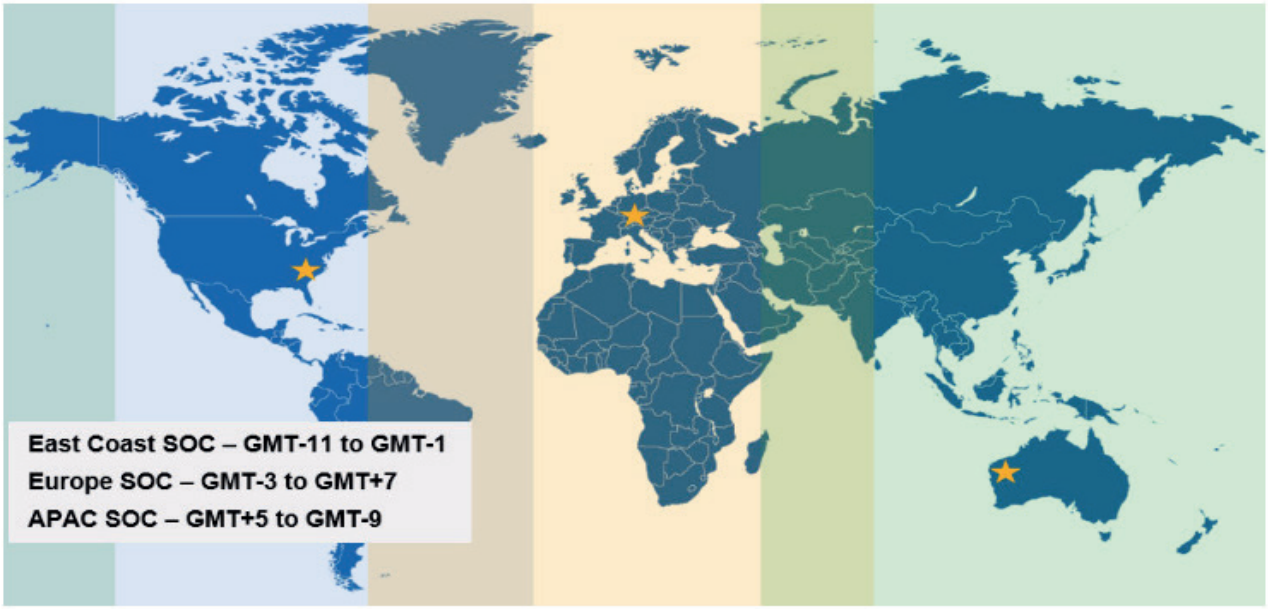
5.3.5.4. A SOC üzemeltetése

Ebben a fejezetben jellemzően a SOC-üzemeltetés humánerőforrás-menedzsment aspektusára fókuszálunk majd. Az informatikai eszközök üzemeltetése IT-üzemeltetési feladatokat takar, speciális ismeretekkel az információbiztonság területén. Egy olyan kardinális fontosságú folyamatos üzemeltetési feladat van, amelyet ki kell emeljünk: ez a SIEM riasztási szabályok frissítése, pontosítása és létrehozása. Tapasztalataink szerint magyar és nemzetközi viszonylatban egyaránt a legnagyobb feladat, ami a SOC dolgozóira nehezedik (inkább második vonaltól vagy mérnöki szinten), az a riasztási szabályok

folyamatos frissítése, finomhangolása az aktuális események, észlelt támadási minták vagy TI alapján. A SOC lelkét adó SIEM sosincsen készen, a riasztásokat generáló szabályoknak folyamatosan követnie kell a változó támadási módszereket. Ez a végtelen versenyfutás jelentős üzemeltetési feladat a képzett kibervédelmi szakembereknek, és nagy stresszforrás is. A szabályokra való hagyatkozáson változtathat az a mostanság kibontakozó trend, ami az UEBA-megoldások elterjedésével, gépi tanulással és prediktív adatelemzéssel igyekszik a manuális szabálybeállítást proaktívan automatizálni.

Az emberierőforrás-menedzsment irányból nézve az üzemeltetési kérdések origója az, hogy a SOC egyik alapvető kritériuma a 24/7-es üzemelés, azaz munkanapokon és hétvégén, éjjel és nappal egyaránt el kell látni a kiberbiztonsági feladatokat. Ennek biztosítására elméleti minimumként 6 emberre van szükség. Azonban ez a valóságban jellemzően nem elegendő. Egyfelől jogi korlátozásai vannak (munkajog, illetve előfordul, hogy nem lehet dolgozó egyedül a munkahelyen). Másfelől a szabadságolásokat, a képzéseket és a váratlan távolléteket is figyelembe kell venni. Sőt, a különböző SOC-feladatokat ellátó szakemberekből is elegendőre van szükség, hogy minden pozícióra jusson kellő számú teljes állásos ember. Ha ezeket is figyelembe vesszük, a minimális üzemeltetési létszám 20 körül állapítható meg, de a gyakorlati minimum sem lehet kevesebb, mint 9 fő (Muniz et al. 2015).

Az üzemeltetés kérdéskörének része, hogy a valóságban a különböző SOC-pozíciók nem egyformán vonzóak, nem egyformán áll rendelkezésre szakember ezekbe. A munkaidőn kívüli műszakok (éjjel, hétvégén) jellemzően kevésbé népszerűek, és az ekkor végzett munka magasabb stresszel is jár, ami a kiégés veszélyét fokozza. Problémák forrása lehet, hogy a normál munkaidőn (hivatali időn) kívül dolgozó szakemberek kevésbé felügyelhetők: a nem a munkájukhoz kapcsolódó tevékenységek így gyakoribbak és nehezebben érhetők tetten. Emellett az ő teljesítményértékelésük is problémásabb a rosszabb láthatóság miatt. A normál munkaidőn kívüli műszakozás miatt a dolgozók egy részének a képzések és csapatépítések szervezése is nehezebb, mivel jellemzően a többséget érintő munkaidőn kívülre esnek, amikor ők vannak szolgálatban. Globális cégek esetében kiváló megoldást nyújthat, ha a FGöld három különböző pontjára telepítenek SOC-csapatokat, amelyek munkaidejükkel, némi átfedést is beleértve, lefedik a teljes glóbuszt és az összes időzónát.



4. ábra

A SOC-csapatok egy lehetséges elosztása a folyamatos üzemelés érdekében

Forrás: Barros–Chuvakin 2016

Azonban a cégek nagy részének ez a megoldás nem reális, méretük vagy költségvetésük miatt. Számukra a munkaerő-menedzsment különböző megoldásainak alkalmazása nyújthat segítséget. A monitorozás ellátása egy kifejezetten nehéz, kevert helyzetét adja a műszakozásnak és a speciális képességekre való igénynek. Az első vonalban (level 1) kezdő elemzők jellemzően fiatalok és kezdők, akiknek a megtartása válik elsődleges problémává, mivel a lehető leghamarabb magasabb pozícióba törekednek, és ennek útja az egyes szervezetek között gyorsabb, mint szervezeten belül. Különösen igaz ez a jelenlegi munkaerőhiányos, kompetitív munkaerőpiacon. A SOC-menedzser feladata a kezdő pozíciók felől érkező, előrelépésre való törekvés helyes kezelése (például a munkakörök rotációjával). Emiatt az állandónak tervezett létszám betöltése a megfelelő szakemberekkel folyamatos kiválasztást és felvételt kell eredményezzen. Megoldások lehetnek a következők:

- Minden SOC-elemző számára tegyen a beosztás lehetővé szabad éjszakákat és szabad hétvégéket.
- Minden elemző számára legyen elérhető képzés és fejlődési lehetőség.
- A munkaköri rotáció előbb említett példája széles körben segíti orvosolni a nyomást a továbblépésre, illetve ezzel jól kombinálja a munkában való képzési lehetőséget is (új munkakörben új képességeket sajátít el).
- Tapasztalt szakemberek is kerüljenek a csapatokba, akik legyenek elérhetőek a kezdő csapattagok számára is.
- A kiválasztás és a munkaerő-felvétel legyen a normál tevékenység része (ehhez lényeges az szakmai kapcsolatrendszer életben tartása).
- Az automatizálás (például gépi tanulás útján) és az eszközök összehangolása segítségével csökkenthetők az unalmas repetitív munkafeladatok, amelyek jelentős stresszforrások.

A SOC teljesítményének mérése fontos része az üzemeltetésnek. Nagyon fontos, hogy a SOC teljesítményét nem az IT-s helpdeskekéhez hasonlóan kell mérni. A információbiztonság speciális folyamatokkal, igényekkel jár, különösen a monitorozás és az incidenskezelés területén. Számos újonnan elterjedt tevékenységre, például a proaktív hunting-ra pedig nincsen még bevett értékelési módszer. A következő teljesítményértékelési mutatókat érdemes figyelembe venni a SOC munkájának értékelése során.

- Riasztásokhoz kötött időmutatók: a riasztástól az első cselekvésig eltelt idő, egyes riasztástípusokra külön is. Ez mérhetővé teszi, hogy a SOC mennyiben tette jobbá és gyorsabbá a fenyegetettségek felismerését.
- Az elemzők teljesítményének mutatói: az egyes elemzők milyen és hány különböző riasztást kezeltek, eszkaláltak. Megmutatja a munkafolyamatok hatékonyságát és annak fejlesztendő területeit vagy éppen sikerességüket.
- A biztonsági incidensekre vonatkozó riasztások metrikái: a különböző detektálórendszerek által létrehozott incidensriasztások száma, a leggyakoribb riasztás- és incidenstípusok, a leghasznosabbnak bizonyult eszközök.

Szintén az értékelés része a SOC tesztelése. Erre jellemzően behatolási teszteket (penetration testing) használnak, amelyek azt ugyan nem bizonyítják, hogy a SOC minden támadást ki tud védeni, de sikertelenség esetén azt biztosan megmutatják, ha esetleg nem látja el kellően a feladatát. A tesztek között lehetnek szimulációs gyakorlatok vagy virtuális tesztek, amelyeket meghatározott időközönként végeznek el.

5.3.5.5. A SOC fejlesztése és bővítése

A már sikerrel megtervezett, beüzemelt és üzemeltetett SOC sincsen véglegesen készen. Ahogy említettük, a szabályok folyamatos karbantartása mindig jelentős erőfeszítéseket igényel, és figyelmet követel az újabb technológiák alkalmazása is az egyre változó támadási módok ellen és a SOC

hatékonyságának fokozására. A Gartner piackutató elemzése szerint (Barros–Chuvakin 2016) a következő években arra lehet számítani, hogy a SOC-kban elterjed a Threat Intelligence (TI), a proaktív hunting szemlélet, többet fognak használni analitikai eszközöket, például UEBA céljára és big data szintű elemzésekre.

A hunting és az adatok feltáró elemzése, fenyegetettségek feltárása a következő jellemzőkkel bír:

- Arra a hipotézisre épül ez az újszerű szemlélet, hogy a fenyegetettségek már jelen vannak a rendszerünkben. A tevékenység egyfajta hipotézistesztelés a rendelkezésre álló monitorozásos adaton, hogy valóban fellelhetők-e a felételezett fenyegetések, felfejthetők-e a szálak ezek mentén egy valódi incidens irányába.
- Ez nemcsak annak elemzését jelenti az adatokon, hogy milyen hibák állnak fenn, hanem azoknak az azonosítását is, amik potenciálisan veszélyt jelenthetnek.

A következő fontos fejlődési irány az eltávolodás a kizárólag riasztásokra épülő folyamatokról:

- Számos korábban is tárgyalt, akár tervezési, akár üzemeltetési nehézség oka, hogy az ember számára feldolgozhatatlanul sok riasztás keletkezik a biztonsági rendszerben.
- A központi dashboardok felületein ezért leginkább csak a legmagasabb kockázati értékű elemeket érdemes megjeleníteni, amihez a legvalószínűbben kapcsolódhat biztonsági incidens.
- Ez utóbbi azt jelenti, hogy egy kockázati pontszámot kell a SOC-ban megjelenő riasztásokhoz kapcsolni, ami a riasztások osztályozását, értékelését is megváltoztatja:
  – a legmagasabb pontszámú riasztások egyből a második vonalhoz (level 2) kerülnek az első vonal bevonása nélkül,
  – az első vonal (level 1) elemzői a listából sorban a legmagasabb pontszámú elemeket veszik le elemzésre, és csak azokat eszkalálják a második vonalba, amik további cselekvést is igényelnek.
- Az automatizálás és az összehangolást biztosító eszközök szerepe megnövekszik. Azonban az automatizálás semmiképp nem lehet még teljes körű: teljesen automatizált SOC-ra nem lehet még számítani. A SOAR (Security Operation, Analytics and Reporting) eszközök alkalmazása segíti ezt az automatizálást:
  – biztonsági üzemeltetési munkafolyamatokat képeznek le, amikkel segíthető az elemzők együttműködése és más csapatszintű folyamatok,
  – az automatizálás és az összehangolás számos, eddig manuális műveletet válthat ki.
- Az álcázásos technikák alkalmazása segíthet megérteni a támadók eszköztárát, taktikáját, a viselkedésüket kontextusba helyezve. Mindeközben álcázásos technikákkal gyengíthető a támadók helyzettudatossága is, azaz félrevezethetők. Ilyen technikák lehetnek a csalik, honeypotok, különösen erősen monitorozott hálózati helyek (amik egyben honeypotok is) stb. Az ilyen csalik alkalmazhatók szervezeten belüli TI előállítására is a megfigyelt támadási próbálkozások elemzéséből.
- Ez utóbbi átvezet a következő trendre, a TI előállításának növekvő elterjedésére. Ahhoz, hogy hatékony Threat Intelligence legyen elérhető, azt elő is kell állítani, és erre a legautentikusabb források maguk a fenyegetettségeknek kitett szervezetek lehetnek. Ez a malware-ek, a lemez- és memóriaképek részletes és alapos elemzését jelenti, amik incidensekhez kapcsolódtak, illetve a támadók profilozására alkalmas szinten kell összegezni a rendelkezésre álló adatokat. Része a más szervezetek által megosztott adatokkal való összesítés, összevetés. És végezetül mindezek eredményeinek jó minőségű, fenyegetettségindikátorok formájában való terjesztése, hogy használhatók legyenek preventív célokra (például SIEM-szabályok kialakítására).
- Az utolsó és egyben majdhogynem szektorfüggetlen trend a fejlett analitikai eszközök egyre nagyobb elterjedése és alkalmazása a kiberbiztonság területén. Ennek leginkább várható alkalmazása az UEBA-megoldások elterjedése lesz. Az ilyen eszközök jellemzően (de nem kizárólagosan) összesített SIEM-adatok utólagos elemzését végzik, kiegészítve a felhasználók azonosítását segítő adatokkal és algoritmusokkal. A prediktív analitikai eljárások (pontosabban

a prediktív, gépi tanuláson alapuló módszerek) lehetővé teszik a szabályalapú riasztásokon való túllépést, és inkább illeszkednek a proaktív hunting stílusú tevékenységekhez. Nem utolsósorban a hatékony predikció leveszi a SOC-személyzet válláról a SIEM-szabályok folyamatos fejlesztésének munkaterhelését, több fókuszt engedve a monitorozásnak és a proaktív védekezésnek.

- Végezetül lényeges trend, hogy a SOC-ok értékelésében jelentős szerep jut a gyakorlatoknak. Ezek során külső (vagy belső) támadóként viselkedő szakértőket kérnek fel, hogy próbatámadást végezzenek, és eközben a SOC teljesítményét értékelik (vörös, kék és lila csapat gyakorlatok).

Összegezve a SOC tervezésről, megvalósításról, üzemeltetésről és továbbfejlesztésről szóló fejezetet, szintén a Grartner (BARROS–CHUVAKIN 2016) elemzésére támaszkodva, öt SOC érettségi szint azonosítható az eszközkészletük alapján.

4. táblázat

A SOC érettségi szintjei

	Jellemző eszközök	Tevékenységek	Hírszerzés/ fenyegetettségkezelés	Értékelési mutatók	Személyzet
1	SIEM	Alapriasztás osztályozása.	Nincs Threat Intelligence.	Nincsenek mutatók.	Riasztás monitorozása (1., 2., 3. vonalban).
2	SIEM és alapszintű hálózati monitorozás	Riasztás osztályozása, tartalom alapján finomhangolás.	Alapszintű TI-adatfolyamok használata.	Alapszintű, eszközközpontú mutatók (például feldolgozott események száma).	Riasztás monitorozása, tartalomfejlesztés (SIEM-szabályok fejlesztése).
3	SIEM, hálózatmonitorozás	Alapszintű anomáliadetektálás, rendszeres behatolástesztelés (penetration testing).	A taktikai és stratégiai hírszerzés szélesebb körű használata.	Eszközközpontú és időalapú mutatók használata.	Alap Threat Intelligence ellátására alkalmas szakemberek is.
4	SIEM, hálózat- és végpontmonitorozás (EDR)	Malware elemzése, alap hunting technikák, vörös és kék csapatgyakorlatok.	Belső TI, taktikai és stratégiai hírszerzés, néhány hírszerzésvezérelt folyamat alkalmazása.	Elemzőhatékonysági mutatók, a jól használható fejlesztésre fókuszálva.	TI-szakember vagy -csapat, „vörös csapat” szakember vagy csapat.
5	SIEM, EDR, NFT, UEBA, álcázásos technikák, SOAR stb.	Monitorozás és válaszadás integráltan, threat hunting, fejlett analitikai eszközök anomáliadetekcióra, lila csapatgyakorlatok.	Belső TI, taktikai és stratégiai hírszerzés, hírszerzésvezérelt folyamatok alkalmazása és TI-adatok megosztása.	Kialakult mutatók a hatékonyságra és teljesítményre, amelyek a detektálás és válaszadás javításán alapulnak.	Hunting csapat, TI csapat, lila csapat.

Forrás: BARROS–CHUVAKIN 2016

Végezetül nemcsak a jó gyakorlatról, hanem a lehetséges buktatókról és kockázatokról is ejtenünk kell pár szót. Jellemző buktató lehet limitált személyi, eszközbeli és anyagi források mellett belevágni a SOC kialakításába. Probléma, ha a SOC szervezeti támogatás nélkül valósul meg, valós céllal, de más csapatokhoz való kapcsolódások nélkül. A hatékony működés gátja az is, ha túl sok riasztás önti el a SOC-ot a különböző (nem feltétlenül helyesen) hangolt eszközökből. Nehézséget okozhat, ha az egyedüli fókusz a SIEM-en van, és nincs rálátás más, esetleg fontos eszközökre, adatokra. A SOC hatékonyságának és jó működésének buktatója lehet, ha a csapat egyedül a riasztások feldolgozására fókuszál anélkül, hogy mélyebb elemzést végezne és átfogó mintázatokat azonosítana. Ez összefügg azzal, hogy ha a szervezet nem tanul az egyedi eseményekből és incidensekből, és nem állít elő TI-adatot, akkor az veszélyt jelenthet a sikerére nézve. Alapvetőbb szervezeti buktató, ha a meglévő NOC (Network Operation Center, amely a hálózatüzemeltetést hivatott ellátni) vagy az IT-helpdesk próbál meg SOC szolgáltatásokat nyújtani. És végül jelentős, fennmaradást veszélyeztető buktató lehet az eddigiekben részletesen tárgyalt munkaerő-megtartás hiánya: ha nincs erre a szervezetnek stratégiája, könnyen elveszítheti a képzett szakembereket és az SOC számára nélkülözhetetlen szaktudást is.

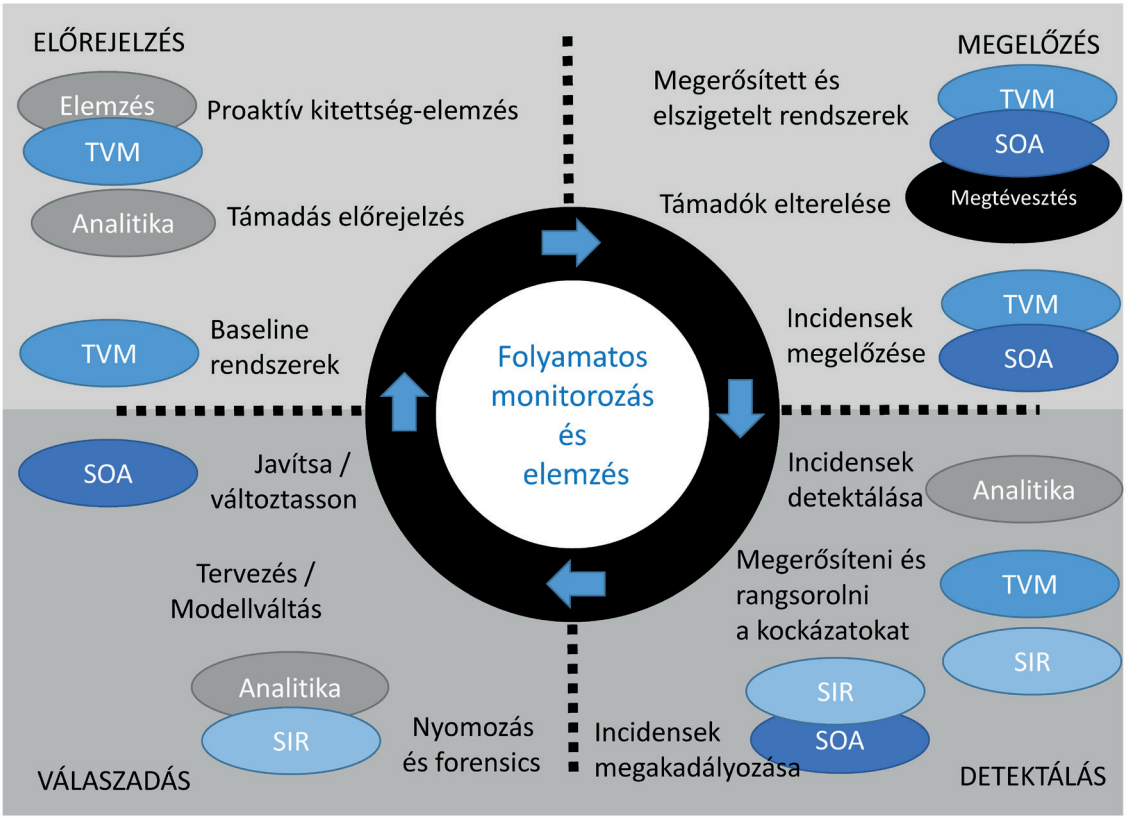
5.4. A TI-vezérelt biztonsági műveleti központ jellemzői

Az SOC-kal kapcsolatos gondolkodást is befolyásolja napjaink kiberbiztonsági szemlélete, amely arra épül, hogy a sikeres támadások elkerülhetetlenek, és valamilyen szinten mindig fennáll a kártékony tevékenység. Ennek okán a SOC-knak a lehető legteljesebb látókörkörre kell törekedniük a monitorozás során. A reaktív helyett proaktív szemléletre van szükség. Tehát nem tartható az a nézet, hogy a SOC mindent megtesz a támadások kivédésére, a védelem pedig a támadások jelére reagál. A támadások ugyanis folyamatosak, és különböző szinten sikeresek is, ezért a cégen belülről és kívülről egyaránt gyűjtött TI-adatokkal a lehetséges támadások elébe kell menni.

Öt ismertető jegyben lehet összegezni a TI-vezérelt SOC jellemzőit:

1. A többféle forrásból származó TI-információt stratégiailag és taktikailag egyaránt használja.
2. Fejlett analitikát (például gépi tanulást) használ arra a célra, hogy megvalósítsa a biztonsági hírszerzést.
3. Amikor lehetőség van rá, automatizáltan működik.
4. Adaptív biztonsági architektúrát alakít ki.
5. A SOC-csapat proaktívan vadászik és nyomoz.

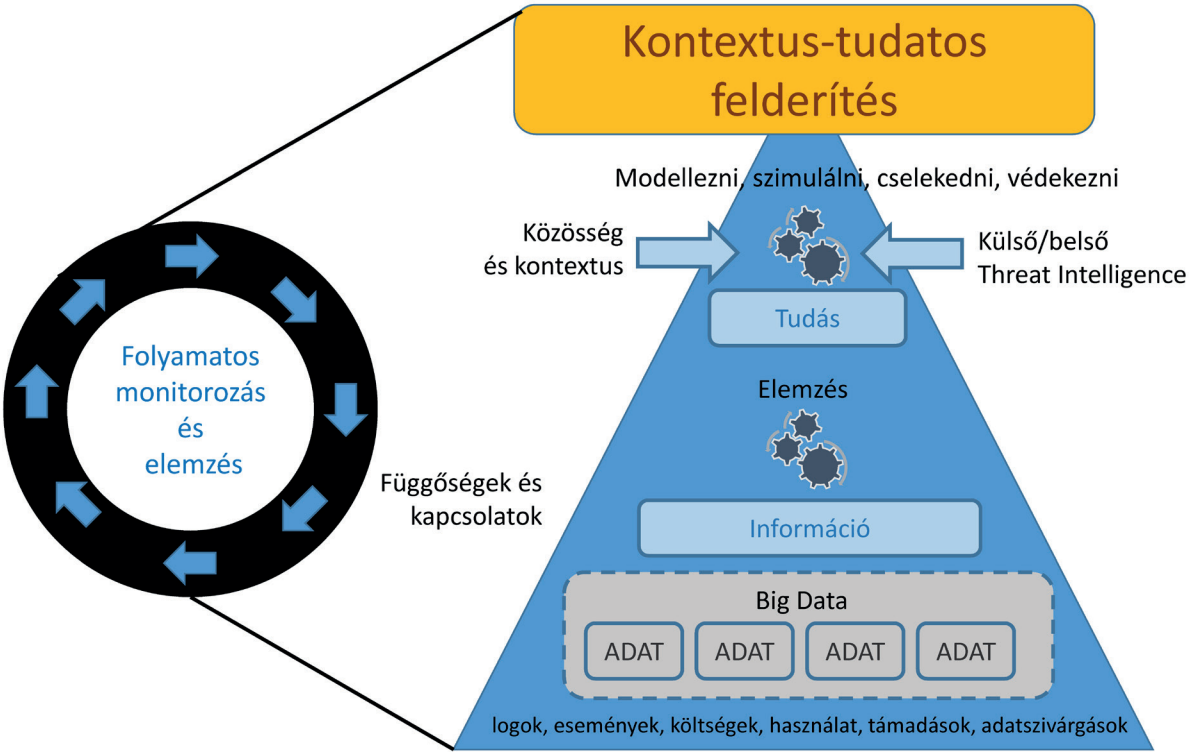
Ez a személet lehetővé teszi a visszajelzésre, tapasztalatokra alapozott alkalmazkodást és fejlődést, amelynek központi eleme a folyamatos monitorozás és elemzés. Ez összekapcsolja a szakembereket, a folyamatokat és a technológiát, ami hírszerzésvezéreltté teszi a SOC-ot (Intelligence Driven SOC, ISOC), ahogy az a következő ábrákon is látszik.



5. ábra

A folyamatos figyelés elemei

Forrás: Rochford–McDonald 2015



6. ábra

A kontextustudatos felderítés jellemzői

Forrás: ROCHFORD–MACDONALD 2015

5.5. A SIEM-ek szerepe a SOC-kban

A biztonsági műveleti központok szíve-lelke technológiai szempontból a SIEM (Security Information and Event Management) alkalmazás. Ez gyűjti, aggregálja, korrelálja a szervezetben fellelhető, biztonsági szempontból releváns adatokat. A korreláció során azokat értelmes mintákba rendezi, amelyeket a SOC-t üzemeltető kiberbiztonsági szakemberek szabályok (SIEM-rules) formájában definiálnak a rendelkezésre álló adatokból és a lehetséges támadási mintázatok alapján. A SIEM a szabályok alapján az elvárt mintázat megjelenésekor riasztást küld az elemzők (SOC analysts) számára, akik 24/7es munkarendben felügyelik a SIEM felületeit, dashboardjait. A riasztások kezelése, ennek dokumentált követése lehetővé teszi az incidensmenedzsment folyamat elvégzését a SIEM-en belül. Végül a támadás irányának rendszeren belüli azonosítása után következhet a védekezés, az elhárítás, az esetleges károk javítása (visszaállítás), amelyek már a SIEM-en kívül történnek. Az incidenskezelés lezárultával a legtöbb SIEM lehetőséget ad a jogi célú dokumentálásra, bizonyítékok gyűjtésére, forensics riportok készítésére.

5.5.1. Naplófájlok (logok)

A SIEM-ek legalapvetőbb adatforrásai a rendszer különböző pontjain gyűjtött naplófájlok, azaz logok. A naplózásban és a naplófájlok beállításaiban az alábbiak az irányadóak (Krasznay 2010): *„A naplóforrásokat úgy kell beállítani, hogy a bejegyzések mindig a megfelelő tartalommal, a megfelelő helyen keletkezzenek és a szükséges ideig legyenek megtartva.* […] *Feltételezve, hogy a logforrás lehetőséget ad a naplózás finomhangolására, a kezdeti beállításokat kellő* körültekintéssel kell megtenni. Előfordulhat ugyanis az, hogy egyetlen forrás olyan mennyiségű adatot generál, amit a felállított infrastruktúra nem

tud kezelni. Ez adatvesztéshez vezethet, lelassíthatja vagy akár teljesen elérhetetlenné teszi a naplózó szolgáltatást, szélsőséges esetben akár a teljes hálózat átviteli sebességére is h*athat. A fenti problémák megelőzése érdekében a naplózást először nem produktív környezetben kell kipróbálni, különösen a leggyakoribb források és a legkritikusabb szolgáltatások esetén. Az egyes gyártók általában tudnak információt adni a naplózással kapcsolatban."* A logok tárolásának kialakítás szintén fontos előfeltétele a sikeres SIEM-használatnak, ezzel a monitorozásnak és az incidenskezelésnek. Krasznay négyszintű tárolást különböztet meg:

- *„Nincs tárolás:* A bejegyzéseknek nincs vagy nem nagy az értékük, ezért nem kell tárolni. Ilyenek lehetnek azok a hibaüzenetek, melyeket csak a szoftver gyártója ért meg, vagy azok a bejegyzések, melyek nem tartalmaznak részletes leírást az eseményről, ezért használhatatlanok.
- *Rendszerszintű tárolás:* A bejegyzéseknek van információértéke, de általában csak az adott rendszer adminisztrátorának, ezért nem érdemes a központi tárba továbbítani. Ezek az információk kiegészíthetik a központi elemzés során feltárt eseményeket, vagy segíthetnek a rendszeradminisztrátornak az általa felügyelt infrastruktúra trendjeinek megértésében és ez alapján az üzemeltetés finomhangolásában.
- *Rendszer- és infrastruktúraszintű tárolás:* Azok az események tartoznak ide, melyek elég érdekesek ahhoz, hogy mind a keletkezés helyén, mind a központi tárban megőrizzék azokat. Jó indok lehet erre a kettős tárolásra az, hogy ha akár a logforrás, akár a központi infrastruktúra sérül, a másikon még megtalálhatók a bejegyzések, vagy ha egy támadás során a támadó megpróbálja eltüntetni a nyomait a naplóállományból, a másik helyen még megtalálhatók a nyomok.

Infrastruktúra szintű tárolás: Általában indokolt legalább két helyen tartani a naplóállományokat, de amennyiben ez nem megoldható, mert például a logforrás tárolókapacitása kicsi, akkor elégséges csak egy központi helyen tárolni." (Krasznay 2010)

Ezenfelül Krasznay ugyanitt helyesen rávilágít arra, hogy *„előre meg kell határozni a logrotálás paramétereit is. Ez azt jelenti, hogy a felgyűlt bejegyzéseket csak egy előre meghatározott méretig vagy ideig kell egy naplóállományban gyűjteni, utána ezt archiválni kell. Így garantálható, hogy mindig lesz szabad tárolókapacitás a naplózáshoz*." A megfelelő mennyiségű, részletességű (verbosity) és elérhető, illetve archivált formában rendelkezésre álló log teszi lehetővé a SIEM hatékony üzemeltetését.

A logokkal kapcsolatban a SIEM mint logaggregáló alkalmazás miatt fontos tisztázni, hogy mely alkalmazások az információbiztonság szempontjából milyen naplózást végeznek. Ennek jó szempontjait adja a *Common Criteria for Information Technology Evaluation* szabvány, amelyben egy teljes úgynevezett család foglalkozik a naplózással kapcsolatos funkcionális követelményekkel, emellett minden egyes biztonsági funkcióhoz meghatározza a naplózandó eseményeket. A szabvány 6 területre osztja a logokkal kapcsolatos tevékenységeket (Krasznay 2010):

- *Automatikus válaszadás:* milyen események következnek akkor, amikor lehetséges biztonsági szabálysértést észlel a rendszer. Ez egyfajta IDS-működést ír elő, ami SIEM-ek esetében kevésbé jellemző, mert ezek ugyan alkalmasak lennének automatikus válaszadásra gyanús események hatására, de a piacon a használatuk még nem elterjedt. Ez az egyik gátja a feltörekvőben lévő *felhasználói viselkedések elemzése* (User Behaviour Analysis, UBA) széles körű használatának a SIEM-ekben.
- *Naplóadatok létrehozása:* meghatározza, hogy milyen típusú tevékenységeket kell rögzíteni, milyen minimális információtartalommal, hogy az jól használható legyen. Ez a funkció hozza létre a naplóbejegyzéseket. A megfelelő beállítású naplóbejegyzések lehetővé teszik a SIEM hatékony alkalmazását, a megfelelő szabályok kidolgozását, illetve az események megértését az elemzők számára.
- *Biztonsági naplóelemzés:* olyan automatikus tevékenységek felsorolása, amelyek segítenek a rendszer tevékenységéből és naplóadataiból kiszűrni a vélt vagy valós biztonsági tevékenységeket. Azaz ez nem más, mint a SIEM alkalmazása naplóadatokon a biztonsági események kiszűrésére (riasztás) és megértésére a hatékony incidenskezelés vagy a forensics eljárás érdekében.

- *Biztonsági naplóadatok áttekintése:* annak meghatározása, hogy milyen módon lehet a jogosult felhasználónak lehetővé tenni a naplóadatok megtekintését. Praktikusan a naplóbejegyzések felhasználói felületére vonatkozó követelmények tartoznak ide. Egyre nagyobb hangsúlyt kap Európa-szerte, így Magyarországon is a személyes adatokhoz való jog érvényesítése a digitális területen. Előfordulhat, hogy a szervezet dolgozói számára átláthatónak, hozzáférhetőnek kell lennie a velük kapcsolatos logoknak, amelyeket kiberbiztonsági célokból gyűjtenek, elemeznek, tárolnak.
- *Naplóesem*ények kiválasztása: azon lehetőségek felsorolása, amelynek segítségével a logok halmazából egy adott tulajdonsággal rendelkező eseményeket ki lehet választani. Gyakorlatilag a riportkészítés követelménye. Ez az előírás lehetővé teszi a SOC szempontjából lényeges jogi eljárásokhoz, a forensics nyomozáshoz használható logok elérését. Jellemzően a biztonsági események egy jelentős részére csak hetek-hónapok elteltével derül fény, így az ekkor is elérhető és kereshető logok jelentik a nyomozás forrását. Abban az esetben, ha valós időben sikerül detektálni egy biztonsági eseményt, annak dokumentálása a logok alapján történik, a releváns logok csatolásával mint bizonyíték.
- *Események tárolása:* a logállományok létrehozásának és tárolásának feltételeivel foglalkozó követelmény, amely a fenti, forensics célú, az eseményt időben később követő elemzést lehetővé teszi. A hosszú időre rendelkezésre álló logok lehetővé teszik mintázatok kiemelését belőlük, hosszan tartó (APT) támadások diktálását, a felhasználói viselkedés elemzését (UBA, amelyhez jelentős előéletre van szükség mint a normális viselkedés alapértéke). Ezekhez a napjainkban elterjedt és elérhető árú *big data* technológiák szolgáltatnak technikai alapot.

5.5.2. Emberi tényezők a SIEM üzemeltetésében

Azonban a logok és adatok csak a sikeres alkalmazás egyik aspektusai (MUNIZ et al. 2015)Operating, and Maintaining Your SOC The complete, practical guide to planning, building, and operating an effective Security Operations Center (SOC. Az emberi tényező központi fontosságú a SOC-kban, és ez a SIEM-ek használatára is igaz.

A hatékony SIEM és a hatékony SOC másik aspektusa a technikai mellett a humán. Az emberi tényező központi szerepet játszik a hatékony riasztási szabályok (SIEM rules) definiálásában: a szakemberek tudása, tapasztalatai és képességei meghatározzák, milyen komplexitású események mintázatait, milyen gyorsan és milyen heterogén adatokra alapozva képesek szabályokba önteni, ezzel riasztani az ilyen támadások esetén, lehetővé téve a hatékony védekezést. Szintén az emberi tényezőn múlik, hogy a SIEM dashboardjait, ahol sok más információ mellett a riasztások is megjelennek, milyen képességű, éberségű, motivációjú elemző szakemberek figyelik. A jó SIEM-elemző képzése és megtartása a szervezetben a SOC-kat érintő munkaerőhiány egyik fő oka, amelytől a későbbiekben sem várható, hogy enyhül (MUNIZ et al. 2015; BARROS–CHUVAKIN 2016). Szintén az emberi tényezőn múlik, hogy a SIEM-et használó, a dashboardjait felügyelő elemző miképp tud hatékonyan együttműködni, csapatban dolgozni más szakemberekkel: malware elemzőkkel, forensics elemzőkkel, szerveradminisztrátorokkal a műszakban vagy a műszakok között, illetve kliensekkel MSSP esetén (lásd bővebben HÁMORNIK–KRASZNAY 2017).

5.5.3. A SIEM működése

A SIEM tehát technológiai támogatást ad a kockázati és biztonsági incidenskezelésben: valós időben összegyűjti, elemzi, ábrázolja vagy bemutatja a különböző, biztonsági szempontból releváns adatokat, valamint az adatok forrásának kontextusát is feltárja (felhasználói, illetve helyi adatokkal gazdagítva, Threat Intelligence információkat felhasználva). Az elemzett adatok felhasználásával készített

jelentések és kimutatások segítségével szintén támogatja az incidenseket követő vizsgálatokat és a biztonsági szabályok betartását ellenőrző tevékenységeket is. A SIEM-technológia alapvető képessége, hogy a széles körű adatgyűjtés különböző forrásaiból és azok elemzéséből képes feltárni, ábrázolni az összefüggéseket. Emellett a megadott szabályok alapján képes a kockázatos eseménymintázatokra riasztásokat adni.

A SIEM-ek összetevői és alapvető képességei összefoglalva a következők:

- *Adataggregálás:* a naplófájlt kezelő rendszer számos adatforrást aggregál, többek között hálózati adatokat, szervereket, adatbázisokat, alkalmazásokat.
- *Korrelálás:* a SIEM közös jellemzőket és kapcsolatokat keres a begyűjtött adatokban ahhoz, hogy értelmes egységekbe rendezze azokat. A korrelálás hoz létre az adatból értelmes információt.
- *Riasztás:* a korrelált események automatikus értékelése alapján riasztásokat küld a beavatkozást igénylő eseményekről. A riasztás kerülhet a SIEM felületére és külső csatornákon keresztül (például e-mail, API) is eljuthat a SOC-elemzőhöz.
- *SIEM dashboardok:* a SIEM összegző felületei, amelyeken az események adatait informatív elrendezésben mutatják be, grafikonok és táblázatok segítségével. Ez lehetővé teszi, hogy esemény- és tevékenységmintázatokat azonosítson az elemző.
- *Előírásoknak való megfelelés:* a SIEM-ek alkalmasak arra, hogy az adott szektort érintő jogszabályi előírásoknak való megfelelés ellenőrzéséhez szükséges adatokat gyűjtsék és összegezzék jelentések, riportok formájában. Ezek alkalmazhatóak tervezési és ellenőrzési (auditálási) helyzetekben.
- *Adatok megtartása:* hosszú távú adattárolók alkalmazhatók arra, hogy a korreláció segítésére régebbi adatok is elérhetőek legyenek, illetve az iparági előírások is meghatározhatnak adattárolási kötelezettséget. A hosszú távú adattárolás elengedhetetlen a biztonsági incidensek későbbi kivizsgálásakor (forensics), mivel az ritka esetnek számít, hogy egy adatlopást például akkor lepleznek le, amikor az történik. Jellemzően napok, hetek, hónapok után derül fény rá, és zajlik le a nyomozás.
- *Forenzikus elemzés (forensic analysis):* a SIEM-ek ezen képessége lehetővé teszi, hogy különböző hálózati elemekhez tartozó naplófájlokat keressenek, időszakokra vagy más kritériumokara szűkítve. Ez megkíméli az elemzőt, hogy nagy mennyiségű logot kellejen áttekintenie és fejben aggregálnia.

További SIEM-képességek, amelyeket érdemes kiemelni:

- Skálázható architektúra és telepítési rugalmasság, ami a nagy, akár globális szervezetek számára is alkalmazhatóvá teszi e megoldásokat.
- Valós idejű adatgyűjtés eseményekről.
- Esemény normalizálása és taxonómia, amely a különböző adatok összekapcsolását teszi lehetővé.
- Incidenskezelés támogatása.

A következő jellemző okok alapozzák meg a SIEM-ek bevezetését egy szervezetben:

- A külső és belső fenyegetések felfedezése.
- A privilegizált felhasználók tevékenységének monitorozása.
- A szerverek és adatbázisok erőforrásához a hozzáférés felügyelete.
- A rendszerek, alkalmazások és a felhasználói aktivitás felügyelete, összehasonlítása és elemzése.
- A szektorbeli szabályozásoknak való megfelelés biztosítása és erről jelentések generálása.
- Támogatás és analízis biztosítása az incidenskezelés munkafolyamatához.

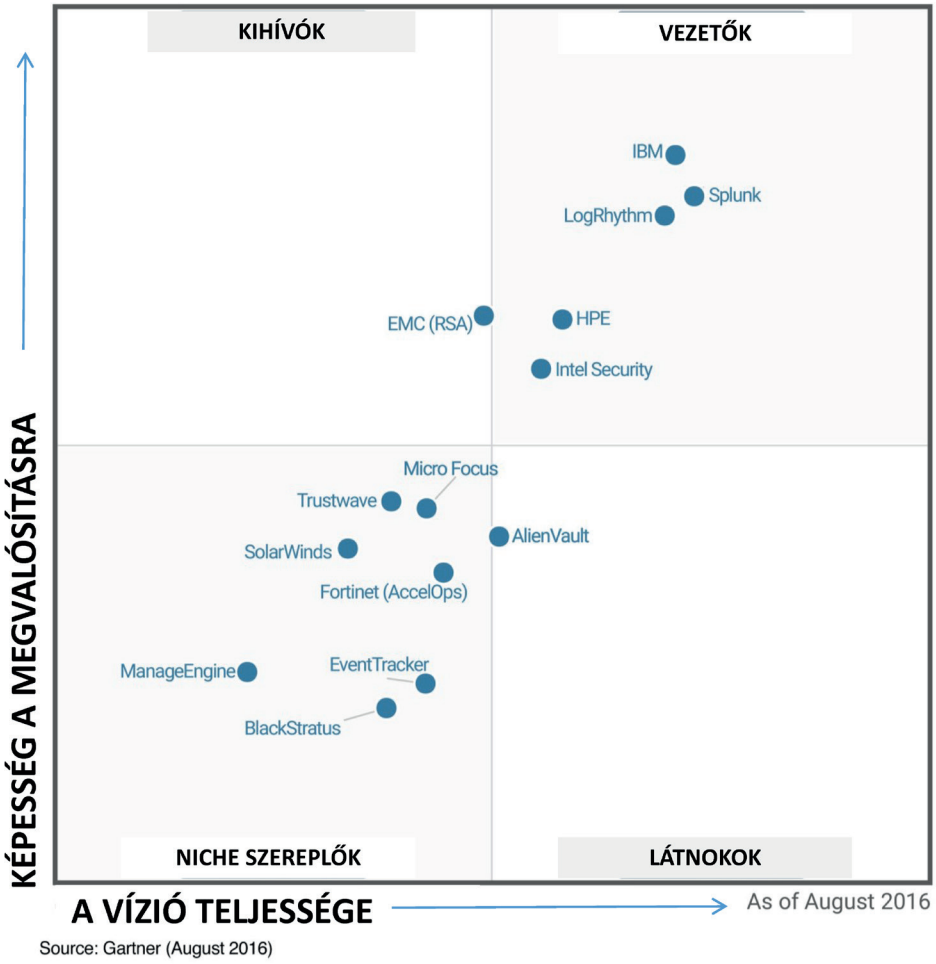
A SIEM-technológia képes összegyűjteni és elemezni az események alatt keletkezett adatokat, amelyek különböző eszközökből, rendszerekből és alkalmazásokból származnak. Az elsődleges adatforrások a logadatok (naplófájlok), azonban a SIEM-technológia képes más formátumú adatok feldolgozására is, amelyek a hálózat környezetében keletkeznek: a felhasználókról, az informatikai eszközökről,

az adatbázisokról, az alkalmazásokról, a fenyegetésekről és a sérülékenységekről. A normalizálás után a különböző forrású adatokat a meghatározott célnak megfelelően lehet elemezni, az összefüggéseket feltárni, úgymint a hálózati biztonsági események felügyelete, a felhasználói tevékenységek nyomon követése, a jogsértések vagy a visszaélések korai felismerése.

5.5.4. A SIEM-piac szereplői

A SIEM-piacon számos kisebb és nagyobb szereplő található meg. Számos specialista, illetve feltörekvő megoldás van jelen a piacon, amelyek egy-egy területen (például felhasználói viselkedés elemzése) kiemelkedő képességekkel bírnak, viszont a nagy szereplőkkel (még) nem veszik fel a versenyt. A Gartner *Magic Quadrant* jó, évenként frissített áttekintést ad a SIEM-piac termékeiről, azok egymáshoz viszonyított helyzetéről és a várható trendekről. Két szempont: a vízió teljessége és az ennek megvalósítására való képessége alapján alkot négy negyedet: vezetők, kihívók, látnokok és székszektorra szakosodott szereplők szerint.

A biztonsági információs és eseménykezelési (SIEM) piacon lévő termékeket a felhasználók az eseményadatok valós idejű alkalmazására, a célzott támadások és adatlopások korai észlelésére, valamint a naplóadatok gyűjtésére, tárolására, elemzésére és jelentésére használják. Emellett fontos alkalmazás az incidenskezelés, a forenzikus elemzés és a jogszabályi előírásoknak való megfelelés is.



7. ábra

A SIEM-piac szereplői

Forrás: Gartner 2016/augusztus

A következő három bemutatott gyártó termékeit az elemzés „vezetők” negyedéből emeltük ki, ami azt jelenti, hogy teljes körű vízióval rendelkeznek, és ennek megvalósítására is minden képességük megvan.

A HPE (ARCSIGHT) jellemzően nagyvállalati SIEM-megoldásként terjedt el. Dinamikus dashboardokkal és eseményvizualizációs eszközökkel rendelkezik. Képes az esemény- és incidenskezelési munkafolyamat teljes mértékű végrehajtására. Támogatja a TI (Threat Intelligence) fenyegetettségi információk fogadását. Hatékony, viszont összetett feladat a telepítése, a kezelése és a fenntartása.

A kevésbé komplex telepítésekhez alkalmazható a HPE ArcSight Express, ami előre definiált felügyeleti szabályokat és jelentéseket, valamint egyszerűsített adatmodellt biztosít, integrálva a SIEM-et, a RepSM TI-t, az IdentityView-t és a csatlakozások kezelését egyetlen hardveren. Az ArcSight átfogó lefedettséget nyújt az előírásoknak való megfelelés, a fenyegetéskezelés és a SIEM use case-ek számára.

Az olyan szervezetek, amelyek nem igényelnek teljes funkcionális eseménykezelést, egyszerűbb és kevésbé drága alternatívát vehetnek igénybe az ArcSight helyett. A HPE biztonsági és műveleti technológiák felhasználói az ArcSight Suite keretei között bővülő számú integrációra és kiegészítőre számíthatnak.

Az IBM (QRadar) – a HPE termékéhez hasonlóan – jellemzően nagyvállalati ügyfelek igényeit szolgálja ki. A termék összetevői egy megoldásba illeszthetők vagy több hardverre szétosztva a funkciókat jól skálázhatók.

A felhasználói viselkedéselemzésnél érdemes kiemelni, hogy az valós idejű és tárolt adatok alapján egyaránt működik. Meghatározza a felhasználók és az alkalmazások alapszintű viselkedését, majd riasztásokat adhat az ettől való eltérésekről.

A QRadar felhasználóorientált tevékenységi jelentéseket és konzolnézeteket nyújt a felhasználók autentikációs tevékenységének valós idejű nyomon követéséhez.

Az elemzés közvetlenül a QRadar elosztott esemény- és adatfolyamából, valós időben és tárolt adatok alapján történik. Kétirányú integrációra van lehetőség az InfoSphere BigInsights (Hadoop) Big Data és az IBM i2 nyomozást támogató elemző alkalmazással.

A termék nagyszámú, előre meghatározott jelentéssablont tartalmaz, amelyek lefedik a legfontosabb előírási követelményeket. Mindezek biztonsági konfigurációval kapcsolatosak, és sebezhetőségi jelentésekkel bővíthetők. Viszonylag egyszerű telepíteni és fenntartani, ami fontos tulajdonsága. Támogatja a fenyegetéskezelés széles körét és a megfelelő use case-eket kisebb és nagyobb léptékű telepítésekhez egyaránt. A biztonságorientált use case-ei a hálózati forgalom elemzésén, a hálózati, szerveralkalmazás használati, viselkedési elemzésén alapulnak.

A Splunk az előző két gyártóhoz képest új szereplő a piacon, egy kiemelkedően rugalmasan alkalmazható termékkel. Erőssége az előre definiált dashboardokban, a keresési képességekben és riasztásokban, a biztonsági monitorozásban és elemzésben, valamint a szabályozásoknak való megfelelés biztosításában rejlik. Erős eszköznek számít, és elterjedt az IT-üzemeltetés területén, sőt az információbiztonság területére ebből az irányból tört be a gyártó.

A SIEM-ként való hatékony alkalmazását lehetővé teszi, hogy a biztonsági eseményforrásokhoz előre meghatározott beállításokat, biztonságspecifikus korrelációs kereséseket tartalmaz, valamit lehetővé teszi a jelentéskészítést és a monitorozást.

Előre meghatározott analitikai dashboardokkal rendelkezik, amelyeken lehetőség van az egyes események mélyebb elemzésére, az elemek (például felhasználónevek, IP-címek, alkalmazások) lépésenkénti kibontására (Drill Down), egészen a nyers adat szintjéig. Mindezt vizualizációk, TI-adatok és metrikák egészítik ki.

A Splunk (más célokra való alkalmazás mellett) SIEM-ként telepítve előre definiált riportokat, dashboardokat, kereséseket, vizualizációkat és valós idejű monitorozást nyújt, amelyek mind a biztonsági, mind a megfelelőségi use case-eket ki tudják szolgálni.

Mellette szól még többek között az adatgyűjtés könnyűsége, az aktív felhasználói közösség és a beállítások széles köre (amelyeket „varázslók” – wizards – is támogatnak).

Nehézséget jelent az alkalmazása során az, hogy több beállítást igényel, mint más SIEM-ek (ami a nagyfokú flexibilitás negatív következménye), és tapasztalt szakember szükséges a hatékony használatához.

Összességében tehát számos kiberbiztonsági use case-t lefed alapbeállításaival, és azok sokféleképp testreszabhatók a megfelelően képzett szakemberek által.

5.6. A SIEM alkalmazása a célzott támadásészlelésre

A szervezetek ellen irányuló kibertámadások egy különösen veszélyes fajtája a célzott támadás (targeted attack), amely a szervezettre szabott, többféle eszközt felhasználó, humán- és technológiai pontokat egyaránt célba vevő kibertámadás.

SIEM-eket a monitorozás javítására továbbra is azért vásárolnak, mert azt gondolják, azok automatikusan, az alapbeállításokkal azonosítják majd a fejlett támadásokat, de ez nem így van. Az előbbiekben leírt szemléletre alapozva folyamatosan szükség van a szaktudásba és a beállítások folyamatos finomításába invesztálni. Ez szükségessé teszi a hunting jellegű proaktív nyomozást, felhasználva a külső és belső TI-információkat, hogy az adatok kontextusba legyenek helyezhetők, és továbbvezessék a hunting-ot.

Olyan előremutató technológiák alkalmazására van szükség, mint az UEBA (User and Entity Behaviour Analitycs), amely a felhasználók és hálózati entitások viselkedését tudja elemezni, illetve az EDR (Endpoint Detection and Response), amely a hálózati végpontok védelmét látja el.

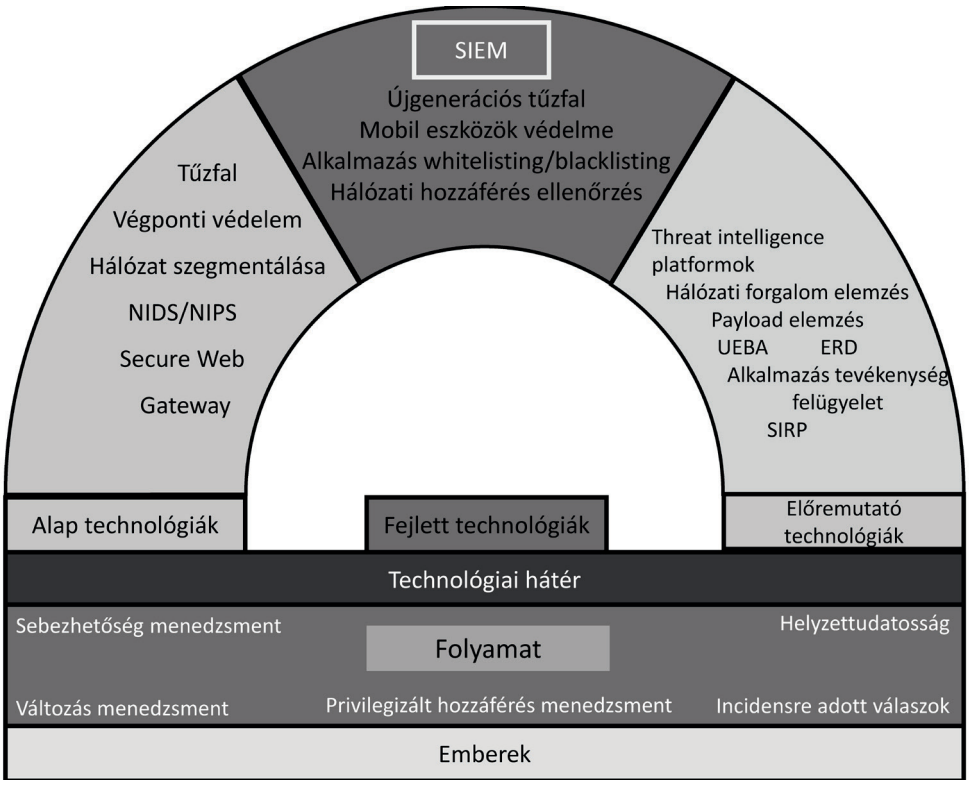
A technológia önmagában azonban nem elegendő. A szakképzett munkaerő, a fejlett technológia és a fenyegetettségekről, a hálózat elemeiről, a használóról szóló kontextuális információ együtt teszi lehetővé a hatékony védelmet. A külső és belső kontextus, a helyzetről szóló, a helyzettudatosságot lehetővé tevő információ lehetővé teszi, hogy a SIEM célozott támadásokat is detektáljon. Ebben fontos kiemelni, hogy a technológia, az eszközkészlet, az információ a szakemberek csapatával együttesen alkot ütőképes SOC-t, amelyet az ergonómia fogalmaival élve jól működő szociotechnikai rendszernek tekinthetünk (Hámornik–Krasznay 2017; Goodall–Lutters–Komlodi 2004).

A technológia szempontjából a célzott támadások ellen hatékonyan támogatja a védelmet az UEBA, a hálózati forgalom elemzése, az EDR, az alkalmazáshasználat monitorozása.

A szakemberek szempontjából a védelemhez a következő képességek és tevékenységek járulhatnak hozzá a leginkább:

- Az elemző képes legyen aktívan keresni a kártékony tevékenységre utaló korai jeleket (hunting). Ezzel a SIEM-et threat hunting és nyomozó platformmá alakíthatja, és nemcsak az automatikusan generált riasztásokra hagyatkozik reaktív módon.
- A tevékenység fókusza a felhasználók, a szerepek, a jogosultságok kezelésének monitorozására kerüljön, ami lehetővé teszi a támadások korai megértését és felfedését.
- A felhasználói tevékenység valós idejű monitorozására van szükség, de legalább a felhasználók szerepeivel kapcsolatos kontextuális információ elérhetővé tételére, hogy az elemző jobban tudja a riasztásokat rangsorolni, és kiválogatni a valóban támadásra utalókat.

Az alábbi ábra a SIEM szempontjából releváns, technológiai folyamatokat és a humán összetevőket foglalja össze a célzott támadások hatékonyabb kivédése érdekében.



8. ábra

A SIEM fő technikai és humán elemei

Forrás: Rochford–MacDonald 2015

Ahogy látható, a viselkedéselemző (UEBA) eszközök kerülnek az SOC-ban üzemelő eszközök hierarchiájának egyik felső, összegző pozíciójába, amely szorosan összekapcsolódik a SIEM-mel. Az UEBA-eszközök lehetővé teszik, hogy rálátás nyíljon a szokásostól eltérő mintázatú felhasználói aktivitásra, a tartalmakhoz és erőforrásokhoz való hozzáférésre, azok használatára. Mindezt egészíti ki kontextussal a TI, így biztosítva a helyzettudatosságot és az ISOC jellegű működést. Mindezek feltétele, hogy a szervezetek elfogadják és alkalmazzák azt a szemléletet, hogy folyamatosan támadás alatt állnak, és ezek valamilyen szinten sikeresek is, így pedig folyamatos válaszlépésekre van szükség, nem pedig kizárólag szabályokra alapozott riasztásokra való reagálásra.

5.7. Megoldások a SOC házon belüli megvalósításának lehetetlensége esetén

Fennállhat az a helyzet (akár időszakosan is), hogy nincs lehetőség a saját, házon belüli SOC kiépítésére. Ennek példái a korábban említett SOC-modellek közül esetlegesen az 1. virtuális SOC (bizonyos eseteiben teljesen MSSP-re bízva) és a 3., az elosztott vagy közösen üzemeltetett SOC.

A külső szolgáltató bevonását a következő okok indokolhatják:

- A megfelelő képzettségű SOC-szakemberek nem állnak rendelkezésre: az ilyen szakemberek toborzása és megtartása egyaránt egyre nagyobb feladatot jelent a rendkívül kompetitív kiberbiztonsági piacon.
- Amennyiben a szervezet SIEM bevezetését tervezi, de még nem jutott el ennek teljes megvalósításáig. Átmeneti megoldásként a cég bevonhat külső szolgáltatót, hogy üzemeltesse a SIEM-et, és így lehetősége van a saját szakembereket a legfontosabb feladatokra csoportosítani.

A szervezet két alapvető utat választhat, amennyiben ezek az okok fennállnak: olyan MSSP-t von be, amely teljesen házon kívülről üzemelteti az információbiztonsági műveleteket. Az első esetben a szervezet az adatait (például a logokat) a szolgáltatónak továbbítja, amelynek szakemberei ezt saját rendszerükön dolgozzák fel, elemzik, felügyelik, majd reagálnak: incidens esetén beavatkoznak, illetve a szolgáltatást igénybe vevő szervezet megfelelő kapcsolattartóján keresztül kiegészítő információt vagy válaszlépéseket kérnek. Ez garantált szolgáltatást jelent (SLA-ban szabályozott rendelkezésre állással), de a szolgáltató szakembereinél hiányzik a cégspecifikus szemlélet, a saját hálózat ismerete („I know my network": GOODALL–LUTTERS–KOMLODI 2004), a szoros kapcsolat a felügyelt hálózat vagy az infrastruktúra üzemeltetőivel (például a változások kezelésének gördülékenyebbé tételére), és költséges lehet a megoldás (szoftverek, szolgáltatások licenszelése), kompromisszumokkal jár a felhasználható adatok tekintetében (például adatvédelmi korlátozások miatt).

A másik megoldás az lehet, hogy valamilyen köztes megoldást választanak, például a SIEM menedzselésének kiszervezését, hogy ezáltal jusson erőforrás olyan dolgokra (például incidenskezelés és válaszadás, az üzleti oldallal való kapcsolattartás, a monitorozás céljainak meghatározása), amik a szervezet számára fontosabbak, speciális tudást igényelnek és megoldhatók saját hatáskörön belül is. Ez lehetővé teszi olyan funkciók ellátását, amikre nincsen szakértelem a szervezeten belül. Emellett egy szolgáltatóval közösen menedzselt SIEM lehetővé teszi a 24/7-es felügyeletet abban az esetben is, ha nincs elegendő saját erőforrás erre: nappali műszakban, hétközben a cég saját csapata végzi a felügyeletet, éjjel és munkaszüneti napokon pedig a partner távolról látja el a SIEM kezelését.

A közösen menedzselt SIEM a kliens oldalán lévő SIEM távoli kezelését, felügyeletét jelenti. Alapszinten ez az elérhetőség, a megfelelő teljesítmény biztosítását, a beállítások és szabályok kialakítását és folyamatos hangolását jelentik. A partner által menedzselt saját SIEM az MSSP által nyújtott szolgáltatással összehasonlítva előnyös abban, hogy nagyobb megbízói kontroll marad a logok, a folyamatok és a tevékenységek fölött, illetve alacsonyabb költséggel és nagyobb rugalmassággal jár.

Specifikusan az alábbi okok alapozhatják meg a közösen menedzselt SIEM-megoldás alkalmazását:

- Törvényi előírás vagy belső szabályozás korlátozza a logok szervezeten kívülre való küldését.
- A biztonsági rendszer architektúrája szempontjából előnyösebb a saját SIEM-alkalmazás használata.
- A költségvetés a SIEM beszerzését preferálja az MSSP-vel szemben.
- A meglévő SIEM nem üzemeltethető kielégítő szinten:
  - a kiberbiztonsági csapat erőforrásai nem teszik lehetővé szakemberek SIEM-felügyeletre való alkalmazását;
  - a csapat kulcsfontosságú szakembere (például SIEM-mérnöke) elhagyta a céget, és amíg az utódjának toborzása, kiválasztása zajlik, egy partner szakembere látja el a feladatait;
  - változások esetén, például amikor a SIEM-alkalmazás nagysága megváltozik, 8/7-es felügyeletről 24/7-re kell átálljanak.

Összességében a közösen menedzselt SIEM alkalmazásának oka lehet az előírásoknak való megfelelés vagy elemzési célok megvalósítása. Amennyiben az a cél a szervezetben, hogy teljesen belső erőforrásokkal üzemeltessék a SIEM-et, akkor efelé a közösen menedzselt megoldás egy praktikus köztes lépés lehet. Ez lehetővé teszi, hogy a kezdetektől (a SIEM telepítésétől) teljes szintű védelmet biztosítson, és a képességek és a tudás a szolgáltató partnertől fokozatosan átkerüljön a saját szakemberekhez.

A megfelelő szolgáltó típusának kiválasztásában segíthet a következő táblázat.

5. táblázat
A szolgáltatók különböző típusai

Szolgáltató típusa	Leírás	Példák szolgáltatóra
Megoldás- és gyártófüggetlen	Tipikusan egy vagy több SIEM-megoldást támogat a házon belüli szakértők és a biztonsági személyzet számára.	Accumuli Deloitte (Vigilant) Optiv
Gyártóspecifikus	Csak saját vagy egy speciális SIEM-megoldást támogat, saját szolgáltatásokat ajánlva hozzá.	EventTracker HP Hurricane Labs (csak Splunk) Trustwave
Több gyártót támogató	A saját megoldásukat támogatják, de azt kiegészítik más, konkurens megoldásokkal is.	IBM

Forrás: Bussa 2015

5.8. Összegzés

A SOC-k egy változó információbiztonsági környezetben kell helytálljanak, a folytonosan megújuló technológiákat integrálva eszköztárukba. Mindezt azért, hogy gyors és hatékony formában tudjanak védekezni az egyre gyakoribb és kifinomultabb támadásokkal szemben. Ennek bemutatására adtuk pillanatképet a jelenleg elterjedt megoldásokról, működési modellekről és technológiákról. Különösen nagy hangsúlyt fektettünk – a technológián és a folyamatokon kívül – a csapatot alkotó szakemberekre, mivel a jelenlegi kiberbiztonsági munkaerőpiacon jelentős verseny zajlik értük. Az idézett és felhasznált irodalomban számos részletesebb technológiai információ is megtalálható a SOC kiépítéséről, üzemeltetéséről, amelyek jó kiegészítései lehetnek jelen anyagunknak.

Felhasznált irodalom

Barros, A. – Chuvakin, A. (2016): *How to Plan, Design, Operate and Evolve a SOC.* Elérhető: http://blogs.gartner.com/augusto-barros/2016/10/17/so-you-want-to-build-a-soc/ (a letöltés ideje: 2017. április 20.)

Bussa, T. (2015): *How and When to Use Co-managed SIEM.* Elérhető: https://www.gartner.com/doc/3112220/use-comanaged-siem (a letöltés ideje: 2017. április 20.)

Goodall, J. R. – Lutters, W. G – Komlodi, A. (2004): *I Know My Network: Collaboration and Expertise in Intrusion Detection.* In: *ACM conference on Computer supported cooperative work,* 342–345., Elérhető: http://doi.org/http://doi.acm.org/10.1145/1031607.1031663 (a letöltés ideje: 2017. április 20.)

Hámornik B. P. – Krasznay C. (2017): *A Team-Level Perspective of Human Factors in Cyber Security: Security Operations Centers.* In: Nicholson, D. (ed.): *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity, July 17–21, 2017, The Westin Bonaventure Hotel, Los Angeles, California, USA,* 224–236., Elérhető: http://doi.org/10.1007/978-3-319-60585-2_21 (a letöltés ideje: 2017. április 20.)

Kavanagh, K. M. – Rochford, O. – Bussa, T. (2016): *Magic Quadrant for Security Information and Event Management.* Elérhető: www.gartner.com/doc/3406817/magic-quadrant-security-information-event (a letöltés ideje: 2017. április 20.)

Krasznay C. (2010): *Naplózás e-kormányzati rendszerekben.* Elérhető: http://krasznay.hu/naplozas-e-kormanyzati-rendszerekben/ (a letöltés ideje: 2017. április 20.)

Muniz, J. – McIntyre, G. – AlFardan, N. (2015): *Security Operations Center: Building, Operating, and Maintaining your SOC (Vol. 2).* Cisco Press. Elérhető: https://books.google.com/books?id=riraCgAAQBAJ&pgis=1 (a letöltés ideje: 2017. április 20.)

Rochford, O. – McDonald, N. (2015): *Five characteristics of an intelligence driven security operation center.* Elérhető: www.gartner.com/doc/3160820/characteristics-intelligencedriven-security-operations-center (a letöltés ideje: 2017. április 20.)

Security information and event management (2017). Elérhető: https://en.wikipedia.org/wiki/Security_information_and_event_management (a letöltés ideje: 2017. április 20.)

6. AZ ESEMÉNYKEZELÉS MŰSZAKI ESZKÖZTÁRA – REFERENCIAARCHITEKTÚRA

Hirsch Gábor

6.1. Az eseménykezelés műszaki eszköztára – referenciaarchitektúra

6.1.1. Bevezetés

Korunk alapvető munkaeszköze a számítógép, alapvető kommunikációs eszköze az internet. Ezen eszközök és adattartalmuk folyamatosan ki vannak téve mind a kívülről, mind a belülről érkező támadásoknak.

Ahhoz, hogy ezeket az információs rendszereket érő támadásokat – incidenseket – megfelelő módon kezeljük, szükséges védendő adataink meghatározása, a védelmi eszközök és szabályok megléte. Ezenfelül a szervezeteket fel kell készíteni egy esetleges támadás felismerésére, kezelésére és az esetleges következmények felszámolására.

A fenti folyamatot több, Magyarországon is elfogadott nemzetközi szabvány is támogatja. Ezek közül a NIST és az ISO 27001 ajánlásai alapján foglaljuk össze a legfontosabbakat.

1. ábra

Az incidensek kezelésének elemei

Forrás: A szerző saját szerkesztése

6.1.2. Az incidenskezelés lépései

- *Azonosítás:* az a lépés, melyben kijelölik azokat az adatokat és infrastruktúraelemeket, amelyek védelme a működés szempontjából szükséges.
- *Védelem:* azon szabályok és tevékenységek összessége, amelyek segítségével az előző lépésben azonosított adatok védelme biztosítható.

- *Felismerés:* a rendszert ért támadás felismerésének folyamata. Ez nem kizárólag véletlenszerűen történik, előre definiált folyamatokkal és adminisztratív intézkedésekkel az esetlegesen még passzív támadások is felismerhetők.
- *Reagálás:* egy kiberbiztonsági eseményre megfelelő intézkedések és tevékenységek végrehajtása, válaszul az észlelt biztonsági incidensre. A folyamatban többnyire adminisztratív intézkedések végrehajtásáról beszélünk, de ez a szükséges műszaki eszközök és technológiák nélkül nem hatékony.
- *Helyreállítás:* az a tevékenység, melynek segítségével a szervezet információs rendszerének normál működése egy incidens után vagy alatt visszaállítható. A helyreállítás a vonatkozó terv alapján történik.

Az alkalmazott műszaki eszközöket incidenskezelési lépésenként mutatjuk be, megemlítve a kapcsolódó adminisztratív intézkedéseket, a szükséges szabályokat is. A téma keretében áttekintjük a szervezeteknek javasolt architektúrákat, a szervezet nagysága, illetve az elvárt rendelkezésre állási szint függvényében.

A rendelkezésre állás az a tényleges állapot, amikor egy informatikai rendszer szolgáltatásai – amelyek különbözőek lehetnek – állandóan, illetve egy meghatározott időben rendelkezésre állnak, és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva. Ebben az összefüggésben jelentősége van az információ vagy adatok rendelkezésre állásának, elérhetőségének is. A rendelkezésre állás értékét százalékosan szokták megadni.

1. táblázat

A rendelkezésre állás szintjei

Rendelkezésre állás szintje	Évi leállás
90%	36,5 nap
95%	18,25 nap
99%	3,65 nap
99,9%	8,76 óra
99.99%	50 perc
99.999%	5 perc

Forrás: A szerző saját szerkesztése

Az incidensmenedzsment műszaki eszköztára – áttekintés

Az incidensmenedzsment azon adminisztratív és technikai intézkedések összessége, amely az információs rendszer megbízható működésének és előírt rendelkezésre állási szintjének biztosítását segíti elő.

Természetesen minden információrendszer működési életciklusában fordulnak elő incidensek, de a megfelelő eszközök és szabályok segítségével minimalizálni lehet azok előfordulását, illetve az elfogadható szinten lehet tartani az incidens okozta károkat.

Ahhoz, hogy lássuk, milyen műszaki eszközök alkalmazhatók az incidensmenedzsment folyamataiban, érdemes megnézni, hogy ezek során milyen adminisztratív és műszaki eszközökkel találkozhatunk, és a szervezetek informatikai rendszerei ezekben milyen fejlettségi szinten helyezkednek el. Az egyes intézkedéseknél a szervezetek fejlettségi szintje meghatározza a biztonsághoz való hozzáállásukat is.

6.1.2.1. Identify

Az azonosítás (Indentify) keretében az alábbi kérdések megválaszolása és megoldása szükséges:

- *Vagyonleltár:* itt meg kell határozni, hogy a rendszerünkről milyen ismeretekkel rendelkezünk. A szervezet informatikai biztonsági szintjétől függően a leltár állapota többféle lehet.
  - Vannak ugyan dokumentációk, de azok megléte és fellelhetősége nem garantált;
  - megtörtént a legfontosabb alkalmazások és a veszélyeztetett adatok azonosítása és dokumentálása;
  - az alkalmazások külső végpontjai, az adatforrások, a hálózati diagram, a külső kapcsolódások és az érintett külső és belső személyzet feladatai dokumentáltak és menedzseltek;
  - azonosították azokat az adatokat, eszközöket, rendszereket, szolgáltatásokat és személyzetet, amelyek lehetővé teszik, hogy a szervezet elérje üzleti céljait, amelyek összhangban vannak a szervezet kockázatkezelési stratégiájával – vagy legalábbis figyelembe veszik azt.
- Üzleti környezet: ebben a pontban a kiberbiztonság és az üzletmenet kapcsolatának meghatározása történik. A szervezetek eltérő módon tekintenek a kiberbiztonság fontosságára az üzleti folyamataikban, ezért a két folyamat kapcsolata eltérő lehet.
  - A kiberbiztonság kezelése nem formalizált, követő, azaz reaktív módú, a fenyegetésekre utólag reagál;
  - biztonsági kockázatértékelés készült, nem a teljes szervezetet átfogóan, csak bizonyos rendszerekre és szigetszerűen;
  - a biztonsági szerepkörök, felelősségek definiáltak, a kockázatértékelés elkészült, dokumentált és ismert a személyzet számára;
  - a szervezet célkitűzése, hogy a feladatok érthetők legyenek az érintett munkatársak részére, pontosan definiálva legyenek a biztonsági szerepkörök, felelősségek és a kockázatkezeléssel kapcsolatos döntések.
- *Irányítás:* a kockázatkezeléssel kapcsolatos politikák, stratégiák meglétének és felhasználásának azonosítása. A lépés során kiderül, hogy a szervezetnek van-e átfogó informatikai szabályozása.
  - A szervezetnek nincs informatikai szabályozása vagy az nem kötődik kockázatértékeléshez;
  - léteznek a vezetés által jóváhagyott informatikai irányelvek, de ezek végrehajtása nem következetes, a szabályozás a magas kockázatú rendszerekre és adatokra összpontosul;
  - kockázattudatos szabályok kialakítása és a végrehajtási lépések gyakorlása a külső és belső partnerekkel egyaránt;
  - a szabályok, eljárások és folyamatok irányítottak és ellenőrzöttek, a szabályozási, kockázati, környezeti és működési követelmények ismertek a biztonsági menedzsment számára.
- *Kockázatértékelés:* a lépésben a szervezet biztonsági szabályainak és tevékenységének azonosítása történik meg. Kiemelt szerepet kap, hogy a kockázatértékelés és az üzleti célok milyen kapcsolatban vannak egymással.
  - A kiberbiztonsági tevékenységeket nem közvetlenül a biztonsági környezet, a szervezeti célok és az üzleti követelmények alapján rangsorolták;

  - a kiberbiztonsági tevékenységeket közvetlenül a biztonsági környezet, a szervezeti célok és az üzleti követelmények alapján rangsorolták;
  - a szervezeti biztonsági gyakorlatok rendszeresek, a tapasztalatok alapján frissített kockázatkezelési eljárásokon alapulnak, amely figyelembe veszi az üzleti célok és a biztonsági környezet, a fenyegetések és a technológia változását;
  - létezik olyan folyamat, melynek során a szervezet a legújabb biztonsági technológiákat és folyamatokat beépíti a kockázatkezelés folyamatába, alkalmazkodva a változó biztonsági környezethez és az egyre bonyolultabb fenyegetésekhez; a kockázatkezelés a teljes szervezetre kiterjed, magában foglalja a tájékoztatást, a kockázatkezelési folyamatokat és a lehetséges biztonsági folyamatokat. A szervezet a biztonsági információkat folyamatosan megosztja partnereivel, hogy a fenyegetettségekről minél pontosabb információkkal rendelkezzenek még az incidens bekövetkezése előtt.
- *Kockázatkezelési stratégia:* ebben a lépésben állapítható meg a szervezet biztonsági fejlettségi szintje.
  - A szervezet kevésbé van tudatában a biztonsági kockázatoknak, nincs szervezeti szintű biztonságirányítás, a kockázatokat még nem azonosították, nincsenek bejáratott folyamatai a biztonsági információk megosztásának és az együttműködésnek;
  - a szervezet tudatában van a biztonsági kockázatoknak, de nincs szervezeti szintű biztonságirányítás, a kockázatokat még nem azonosították; vannak folyamatai, de nem képes az információk megosztására partnereivel;
  - a szervezet rendelkezik átfogó biztonságirányítással, érti, hogy függ a partnereitől kapott biztonsági információktól, melyeket megkap és felhasznál a szervezeten belül a kockázatkezelési döntések során;
  - a kockázatkezelés a teljes szervezetre kiterjed, magában foglalja a tájékoztatást, a kockázatkezelési és a lehetséges biztonsági folyamatokat; a szervezet kezeli a kockázatokat, és a biztonsági információkat folyamatosan megosztja partnereivel, hogy a fenyegetettségekről minél pontosabb információkkal rendelkezzenek még az incidens bekövetkezése előtt.

Az azonosítási folyamat támogatására használt *műszaki eszközök* elsősorban az információk megosztását, az azokhoz való megfelelő hozzáférést segítik elő. A folyamatban a biztonsági gyakorlatok elvégzéséhez szükséges informatikai infrastruktúra mint műszaki eszköz fontos szerepet kap. A gyakorlatok során a szimulált biztonsági eseményt nem a szervezet napi működését biztosító, éles adatokkal rendelkező rendszereken végzik, hanem speciálisan tesztelési célra összeépített, az éles rendszerrel megegyező felépítésű, jogosultságú és frissítési állapotú tesztrendszereken.

6.1.2.2. Protect

A védelem (protect) fázis már olyan aktív intézkedéseket és eszközöket tartalmaz, amelyek az informatikai rendszer védelme szempontjából rendkívül fontosak. Az ezzel kapcsolatos feladatok az alábbiak.

- *Hozzáférés-szabályozás:* az a folyamat, melyben a szervezet a felhasználók jogosultságait meghatározza, beállítja és ellenőrzi.
  - Az eszközökhöz való hozzáférés nincs korlátozva vagy naplózva;
  - a kritikus vagy érzékeny adatokat tartalmazó rendszerekhez korlátozott a hozzáférés, és ezt naplózzák is;
  - az összes eszközhöz és felszereléshez csak a jogosult felhasználók férhetnek hozzá, és ezt naplózzák is;
  - az eszközökhöz és kapcsolódó létesítményekhez való hozzáférés csak a jogosult felhasználók, tevékenységek és folyamatok számára engedélyezett, a hozzáférési naplókat pedig rendszeres időközönként ellenőrzik.

- *Tudatosság és képzés:* az incidenskezelés fontos alapköve a felhasználók biztonságtudatosságának növelése és a szakszemélyzet képzése az esetlegesen előforduló incidensek kezelésére.
  – Nincs képzés az alkalmazottak és partnerek számára;
  – rendszeres biztonsági képzés az alkalmazottak részére az érzékeny adatok és rendszerek felhasználásáról;
  – rendszeres kiberbiztonsági képzés a munkavállalók részére, és az üzleti partnerekkel szemben is ez az elvárás;
  – a szervezet a személyzetének és a partnereinek is biztosít biztonságtudatossági oktatást, ezáltal kellőképpen gyakorlottak az információbiztonsági feladatokban, összhangban a vonatkozó szabályokkal és folyamatokkal.
- *Adatbiztonság:* az adatok kezelésének fontos tulajdonsága a szervezetek ezzel kapcsolatos fejlettségi szintje.
  – Az adatbiztonsággal kapcsolatos tevékenységek nem következetesek sem a szervezeten belül, sem pedig a partnerekkel kapcsolatban;
  – az adatcsere során az érzékeny adatok titkosítva vannak;
  – az adatcsere során az érzékeny adatok titkosítva vannak, és megfelelő megállapodások vannak minden olyan partnerrel, amelyek hozzáférnek ezekhez az adatokhoz;
  – az adatok és információk kezelése összhangban van a szervezet kockázatkezelési stratégiájával, amely biztosítja az adatok bizalmasságát, sértetlenségét és rendelkezésre állását.
- *Információvédelmi folyamatok és eljárások:* az informatikai rendszer védelme a szervezetek kiemelt feladata, figyelembe véve, hogy fontos adataik ezen rendszerekben találhatók meg.
  – Nem érvényesítenek biztonsági szabályokat;
  – az érzékeny adatoknál és a kritikus rendszereknél a szervezet biztonsági szabályokat alkalmaz;
  – a szervezet biztonsági szabályokat alkalmaz a szervezeten belül és az üzleti partnerek felé;
  – a biztonsági szabályok, eljárások és folyamatok definiáltak, és a szervezet alkalmazza is ezeket az informatikai rendszerek és eszközök védelmére.
- *Karbantartás:* az informatikai rendszerek frissítése és karbantartása fontos része az informatikai biztonságnak, alapvetően a rendelkezésre állást segíti elő, de a nulladik napi fenyegetések egy részét is javíthatja.
  – Az információs rendszer elemeinek javítása és karbantartása nem rendszeres;
  – az érzékeny adatokat és kritikus rendszereket működtető informatikai infrastruktúra elemeit folyamatosan karbantartják, és ezek naprakészek;
  – az informatikai infrastruktúra elemeit folyamatosan karbantartják, és ezek naprakészek;
  – az ipari ellenőrző és információs rendszerek elemeinek karbantartása és javítása összhangban van a vonatkozó szervezeti szabályokkal és eljárásokkal.
- *Védelmi technológiák:* a szervezetek által alkalmazott védelmi megoldások és szoftverek összességét soroljuk ebbe a csoportba, melyek a vonatkozó szabályokkal összhangban alkalmazva az információvédelem fontos alapkövei.
  – A szervezet általános biztonsági szoftvereket használ (vírusvédelem, kéretlen és adathalász leveleket ellenőrző eszközök);
  – a biztonsági megoldások kockázat alapján működnek, szervezeten belül;
  – a biztonsági megoldásokat következetesen alkalmazzák a szervezeten belül és az üzleti partnereknél is;
  – a rendszerek és eszközök ellenállóképességének növelésére alkalmazott technikai védelmi megoldások a vonatkozó szabályokkal, eljárásokkal és megállapodásokkal összhangban működnek.

A folyamatban alkalmazott műszaki eszközök köre már jóval szélesebb, mint a megelőző folyamat során.

Jogosultságkezelés: bármely szabványos informatikai rendszerben megvalósítható a felhasználók jogosultságának szerepkör alapú kezelése. Ennek következtében a felhasználók csak azokat az adatokat láthatják és azokat az erőforrásokat használhatják, melyekre szerepkörük alapján jogosultak. A jogosultságkezelés másik módja a dinamikus hozzáférés-vezérlés, amikor az adattartalom vagy az adatok egyes tulajdonságai alapján határozható meg a felhasználók hozzáférése.

Naplózás: a jogosultságkezelés és a fájlhozzáférés ellenőrzésére is használható eszköz. Az informatikai rendszerek mindegyike rendelkezik valamilyen szintű naplózással. Az operációs rendszerekben a biztonsági naplózás beépített szolgáltatás. Az informatikai rendszerek alapértelmezetten körkörös naplózást alkalmaznak, amelynek következtében a naplóesemények meghatározott időközönként felülíródnak. A naplózás részletességét, a naplóállományok mentését és megőrzési idejét az érintett informatikai rendszer besorolása határozza meg.

Naplóelemzés: az informatikai rendszer különböző elemeiről begyűjtött naplók kezelését és ellenőrzését jelenti. Az eszközök általában olyan mennyiségű naplót generálnak, amelyek elemzése kizárólag elektronikus eszközökkel oldható meg. Ezek az eszközök képesek arra, hogy az egymásból következő naplóeseményeket korrelálják (összevonják), és már csak a naplóeseményt kiváltó tevékenységről küldjenek riasztást. A naplóelemzés célja lehet az események rekonstrukciója vagy azok bekövetkezésének megelőzése. Ez utóbbi esetben a naplóelemzés egy kifinomultabb folyamat.

Titkosítás: az adatok olyan átalakítása, amely illetéktelen személy számára az adatot értelmezhetetlenné teszi. Az informatikai rendszerekben többnyire szimmetrikus kulcsú titkosítást alkalmazunk, mert annak megvalósítása egyszerűbb és gyorsabb. Az aszimmetrikus kulcsú titkosítást nagyrészt a kulcsok cseréjére használják fel.

Vírusvédelem: a szervezeteknél szabványos, kereskedelmi forgalomban kapható eszközökkel oldják meg. A vírusvédelmi szoftverek a fenyegetéseknek csak bizonyos hányadára képesek reagálni, azt is általában késéssel. Nagyobb szervezetek esetében fontos, hogy a vírusvédelmi szoftver központilag menedzselhető és naplózható legyen.

Antimalware: az informatikai rendszereket nem kizárólag vírustámadás érheti, hanem számos egyéb támadási lehetőséget tartunk nyilván, amelyeket úgynevezett kártékony kódok képesek a rendszerünkben végrehajtani. Ezeket a kártékony kódokat a vírusvédelem nem minden esetben kezeli, elvégre nem vírusok, viszont alkalmasak arra, hogy a védett információkat kiküldjék egy előre definiált helyre vagy támadó hálózat tagjává tegyék az informatikai rendszer elemeit. Ezek ellen nyújt hatékony védelmet az antimalware program.

Frissítések: az informatikai rendszerek működtetésének alapvető szabálya a megfelelő frissítések alkalmazását írja elő. A frissítések amellett, hogy funkcionális bővítést is tartalmazhatnak, a rendszerek biztonsági sérülékenységeinek egy részét is képesek javítani. Frissíteni nem csupán az alkalmazott operációs rendszereket és a vírusdefiníciós adatbázisokat, hanem az egyéb, a rendszerben alkalmazott szoftverkomponenseket is szükséges.

6.1.2.3. Detect

A felismerés (detect) fázisban az informatikai rendszerben meglévő anomáliákat keressük, amelyek segítenek felismerni a rendszert ért támadást. Az itt végrehajtható feladatok az alábbiak.

- *Anomáliák és események:* a lépés keretében az információs rendszer szokásos működése során figyelik az eseményeket. Amennyiben egy észlelt esemény eltér a rendszer szokásos viselkedésétől, az biztonsági eseményre utalhat.
  - A problémákat általában ismert biztonsági támadások okozzák;
  - a szervezet az érzékeny adatok és rendszerek rendellenes viselkedését időben észleli;
  - a szervezet a rendellenes viselkedést időben észleli;
  - a szervezet időben észleli a rendellenes viselkedést, és tisztában van az események potenciális hatásával.
- *Biztonság folyamatos figyelése:* az informatikai rendszerek kapcsán minden esetben felmerül azok felügyelete, illetve a felügyelet eszközei és szabályrendszere. Felügyelt rendszerek esetében mindig nagyobb az anomáliák észlelésének valószínűsége.
  - Ha van monitoringrendszer, de az nem menedzselt;
  - a magas kockázatú adatok és rendszerek felügyeltek és menedzseltek;
  - az informatikai eszközök és alkatrészek felügyeltek, a szervezetben rendszeresen ellenőrzik a biztonsági eseményeket;
  - az informatikai eszközök és alkatrészek felügyeltek, a szervezetben rendszeresen ellenőrzik a biztonsági eseményeket a védelmi intézkedések hatékonyságának ellenőrzésére.
- *Felismerési folyamatok:* szintén a rendszerek üzemszerű működéséről eltérő működést és hozzáférési kísérleteket figyeli.
  - Érzékelő rendszerek kialakítása nem következetes és nincs tesztelve;
  - az érzékelő rendszereket az érzékeny adatokon és rendszereken rutinszerűen kialakítják;
  - az érzékelő rendszereket kialakították és frissítik az ismert fenyegetések alapján;
  - az érzékelési folyamatokat és eljárásokat kialakították és tesztelik, így megfelelő időben érzékelik a rendellenes viselkedést.

A folyamatban használt műszaki eszközök köre *kifejezetten az észlelést támogatja.* Ezek az alábbiak.

Naplózórendszer: a naplózórendszerek összegyűjtik az informatikai rendszerben a működés során keletkező esemény- és biztonsági naplókat, azaz az ezzel kapcsolatos bejegyzéseket. Ennek alapján a naplók képet adnak az informatikai rendszer „egészségi állapotáról", illetve a rendszeren belül a biztonsági eseményekről. A biztonsági események naplózásakor a sikeres és sikertelen hozzáféréseket, az alkalmazásindítási és eszközelérési kísérleteket érdemes naplózni. Az informatikai rendszerek majd minden eleme képes naplózásra, a naplózási paraméterek, illetve a naplózandó események köre beállítható, ahogy az is, hogy a naplóállományokkal mit tegyen a rendszerelem.

Naplóelemző rendszer: az informatikai eszközök által begyűjtött naplók az eszközökön találhatók meg. Ezek összegyűjtése és korrelációja a naplóelemző rendszer feladata. Egy biztonsági esemény több eszközön generál egymástól független eseményeket, melyeket külön-külön nem lehet kezelni. A naplóelemző rendszerekkel ezek az események összevonhatók, azok eredeti forrása megállapítható.

IPS/IDS-rendszerek: a külső támadások elleni védelem eszközei. A teljes hálózati forgalom átfolyik rajtuk, amelyben azokat a jellemző folyamatokat keresik, amelyek biztonsági incidensre utalnak. Fontos, hogy ezek a rendszerek nem csupán a forgalom folyamatos elemzését végzik, és szükség esetén riasztanak, hanem képesek az adott folyamatot letiltani, megakadályozva ezzel a rendszer illetéktelen elérését.

6.1.2.4. Respond

A reagálás (respond) fázisban az esetlegesen bekövetkezett biztonsági esemény kezelését, rövid távú következményeinek felszámolását végezzük.

- Reagálási terv: a reagálási terv egy olyan előre definiált szabálygyűjtemény, melyben a szervezet szabályozni tudja a vészhelyzeti protokollt, elkerülve ezzel, hogy egy esetleges incidens esetén a választevékenységek kárt okozzanak.
  - Nincs előre definiált reagálási terv;
  - reagálási terv készül a kritikus adatokkal és rendszerekkel kapcsolatosan;
  - szervezeti szintű reagálási folyamatot dokumentálnak és ismertetnek a személyzettel;
  - a reagálási folyamatok és eljárások végrehajtásra vannak kidolgozva, hogy a biztonsági eseményeket megfelelő időben észleljék.
- Irányítás a reagálás fázisban: az irányítás az incidens elhárításának irányítását jelenti, mely eltérhet a szervezet normál működése során alkalmazott irányítási struktúrától.
  - A szervezetnél reaktív (követő) irányítás van;
  - a szervezetnél tervszerű irányítás van;
  - az üzleti partnerekkel összehangolt irányítás van;
  - az irányításai folyamatok a külső és belső érdekeltekkel összehangolt módon, adott esetben a külső bűnüldöző szervek támogatásával történik.
- Elemzés: az incidens kezelése során folyamatosan elemezni kell a beérkezett adatokat, ennek alapján pedig finomítani a válaszlépéseket.
  - Nincs hivatalos elemzési folyamat;
  - az elemzés az adat érzékenységén alapul;
  - az analízis átfogó, minden rendszert érint;
  - folyamatos elemzés a megfelelő reagálás és a helyreállítási tevékenységek támogatására.
- Kárenyhítés: a lépésnek szintén az incidens bekövetkezését követően van szerepe, amikor a rendszerben tapasztalt károk minimalizálására törekszik a szervezet.
  - A szervezetnek a kárenyhítésre kevés lehetősége van;
  - a szervezet az érzékeny adatok és rendszerek veszteségét, illetve az azokhoz való hozzáférést korlátozni tudja. Megfelelő dokumentációval rendelkezik a gondatlanságok elkerülésére;
  - a korai felismerés lehetővé teszi a megfelelő válaszlépéseket a károk enyhítése érdekben;
  - a szervezetben olyan folyamatok zajlanak, melyek megakadályozzák a biztonsági esemény kiterjedését, a káros hatások csökkentése és az incidens következményeinek felszámolása érdekében.
- Fejlesztések: a reakciók fejlesztése fontos lépés a folyamatban. Minden esemény kezelése új, korábban nem ismert vagy alkalmazott reakciókat követel meg, így mindenképpen fejleszteni érdemes a szervezeteknek a reagálási képességüket.
  - A fejlesztések nem folyamatosak, csak biztonsági incidenseket követően történnek;
  - az érzékeny adatok és rendszerek biztonsági megerősítése megtörtént;
  - biztonsági rések elfordulnak, de a szervezet gyakorlata lehetővé tette az incidens felismerését és kezelését;
  - a szervezeti reakciók közé beépítésre kerülnek az aktuális és a korábbi biztonsági eseményekre adott reakciók tanulságai.

A folyamatban alkalmazott műszaki eszközök kifejezetten a biztonsági események következményeinek felszámolását segítik. Ezek az alábbiak lehetnek:

Naplóelemzés: az informatikai eszközök által begyűjtött naplók az eszközökön találhatók meg. Ezek összegyűjtése és korrelációja a naplóelemző rendszer feladata. Egy biztonsági esemény több eszközön

generál egymástól független eseményeket, melyeket külön-külön nem lehet kezelni. A naplóelemző rendszerekkel ezek az események összevonhatók, azok eredeti forrása megállapítható.

Tűzfalak: a tűzfalak a külső támadások ellen védik a szervezeti infrastruktúra elemeit. A tűzfal beállításai lehetővé teszik, hogy a rendszer csak bizonyos protokollokon keresztül legyen kívülről elérhető, mellyel szűkíteni lehet az esetleges támadások körét. A tűzfalak alapvetően ismert, szabványos módon érkező fenyegetések elhárítására alkalmasak.

IPS/IDS rendszerek: ezek a rendszerek a külső támadások elleni védelem eszközei. A teljes hálózati forgalom átfolyik rajtuk, melyben azokat a jellemző folyamatokat keresik, mely biztonsági incidensre utal. Fontos, hogy ezek a rendszerek nem csupán a forgalom folyamatos elemzését végzik, és szükség esetén riasztanak, hanem képesek az adott folyamatot letiltani, megakadályozva ezzel a rendszer illetéktelen elérését.

Hálózati szegmentáció, rendszerek izolálása: a technika lényege, hogy a különböző funkciójú infrastruktúra elemeket egymástól hálózati eszközök segítségével elválasztják, és tűzfalszabályok segítségével csak a kommunikációhoz feltétlenül szükséges portok kerülnek megnyitásra. Természetesen az érzékeny adatokat kezelő infrastruktúraelemek légréssel is leválaszthatók a többi hálózati szegmensről.

6.1.2.5. Recover

A helyreállítás (recover) fázisban az informatikai rendszer működőképességének helyreállítása történik, az ehhez szükséges lépések az alábbiak.

- Helyreállítás tervezése: a szervezet informatikai rendszereinek elemei egymásra épülnek, ezért azok helyreállítása nem működik ad hoc módon. Azt tervezetten, a helyi sajátosságok ismeretében érdemes megtenni.
  - A helyreállítási eljárások külső szállítóktól függenek;
  - az érzékeny adatok helyreállítása tervezett és irányított;
  - az üzlet számára kritikus rendszerek és kapcsolatok helyreállítása tervezett és irányított;
  - a helyreállítási folyamatok végrehajtása és fenntartása biztosítja a kiberbiztonsági esemény által érintett rendszerek működésének megfelelő idő alatt történő helyreállítását.
- Helyreállítás fejlesztése: a szervezetnek a helyreállítási folyamatot folyamatosan fejlesztenie kell, és azt napra készen kell tartania a folyamatok hatékonyságának megőrzése érdekében.
  - A fejlesztés a gyártók ajánlásain alapul;
  - az érzékeny adatok helyreállítási terve értékelt;
  - a helyreállítási terveket értékelni kell, hogy azok követhetők legyenek;
  - a helyreállítási tervezést és a folyamatokat folyamatosan fejlesztik a tanulságok beépítésével.
- Helyreállítási kommunikáció: a rendszerek helyreállítása során a kommunikáció és az irányítás elengedhetetlen.
  - A helyreállítás nincs irányítva;
  - a visszaállítási folyamatokat belülről irányítják;
  - a visszaállítási folyamat az üzlettársakkal közösen irányított;
  - a helyreállítási folyamat külső és belső partnerek irányításával – például irányítási központ, internetszolgáltató, támadó rendszerek tulajdonosai, áldozatok stb. – történik.

A recovery fázisban alkalmazott műszaki eszközök a rendszerek működésének mielőbbi helyreállítását szolgálják. Ezek az alábbiak:

Redundáns adattárolás: a szervezetek adatait az informatikai rendszerekben alapértelmezetten redundánsan, azaz „több példányban” tároljuk. Az adatok tárolása során mindig valamilyen RAID megoldást alkalmazunk. Azt, hogy a rendelkezésre álló redundáns tárolási lehetőségek közül melyiket választjuk, a szervezet mérete, a rendelkezésre álló informatikai infrastruktúra és az előírt rendelkezésre állási szint határozza meg.

Mentés: a mentés a mentési tervben meghatározott rendszerelemek és adatok másolatának tárolását jelenti egy elkülönült rendszerben vagy adathordozón. A mentéseket meghatározott terv alapján készítjük, mely lehetővé teszi az adatok minél frissebb, a biztonsági eseményt megelőző állapotának helyreállítását.

Helyreállítási teszt: a helyreállítási teszt a mentésekkel és a mentési stratégiával szoros összhangban működő folyamat. Ezt a mentési folyamat javítására, a helyreállítás időszükségletének pontosítására használjuk. A helyreállítási teszt során egy vagy több rendszer elemeit vagy adattartamát kell a mentések segítségével megadott kiinduló állapotú hardverelemeken helyreállítani.

Vészhelyzeti tartalék eszközök/rendszerek: a szervezetek informatikai infrastruktúrájának rendelkezésre állási szintje minden esetben elő van írva. A rendelkezésre állási szint azt határozza meg, hogy a szervezet rendszerében mekkora az az időintervallum, amíg a rendszerek kiesése nem okoz elviselhetetlen üzleti károkat. Ennek függvényében alkalmazhatunk vészhelyzeti tartalékeszközöket vagy -rendszereket. A vészhelyzeti tartalékeszközök többnyire úgynevezett hideg tartalékok, melyek dobozban állnak a raktárban, de a biztonsági esemény bekövetkezését követően könnyen hozzáférhetők, és a visszaállítási tervben meghatározott idő alatt üzembe helyezhetők. Alkalmazhatunk még meleg tartalék rendszereket is. Ezek az eszközök vagy rendszerek folyamatosan működnek, be vannak építve az informatikai rendszerbe. Általában kétféle üzemmódban használják őket:

- failover: ez az eszközöknek egy olyan felhasználása, amikor az informatikai rendszer azonos funkciójú elemeiből két vagy több példány folyamatosan működik a rendszerben, de egyidőben mindig csak egy érhető el belőle. Ilyenkor ezek az eszközök folyamatosan monitorozzák egymást, és amikor az élesen működő valamiért megáll, azonnal a helyére lép a működő tartalék. Ezt a váltást általában a felhasználók nem veszik észre, annyira rövid idő alatt megy végbe.
- load balancing: az informatikai rendszer azonos funkciójú elemeiből ebben az esetben is kettő vagy több darab működik a rendszerben, de az eszközök mindegyike folyamatosan elérhető a felhasználók számára. A felhasználói kérésekre a redundáns rendszerek közül mindig válaszol valamelyik. Így az eszközök egyikének a kiesése esetében kizárólag a megnyitott folyamat veszik el, de ezt az operációs rendszerek kiküszöbölik, tehát a felhasználó számára nem észrevehető. A megoldás nagy előnye, hogy sokkal nagyobb felhasználószámot képes kiszolgálni, mint a failover.

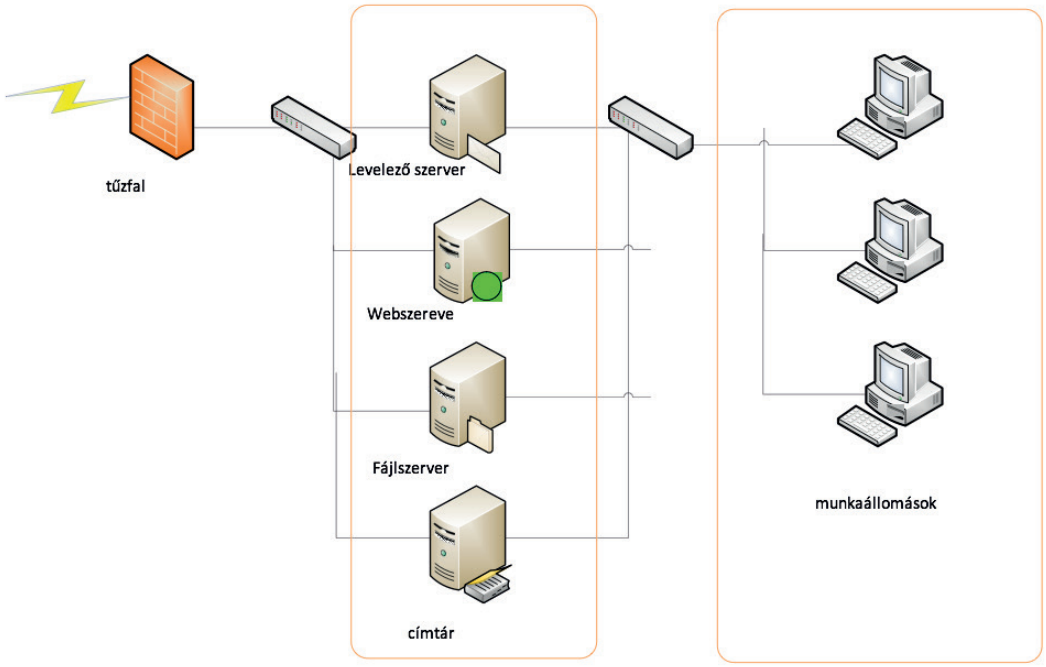
Disaster recovery site: vannak olyan kritikus rendszerek és infrastruktúrák, melyek kiesése a szervezet számára nem tolerálható, ezért gondoskodni kell arról, hogy ezek folyamatosan elérhetők legyenek. Erre használható ez a technika. A disaster recovery site az informatikai rendszer egy olyan része, mely attól fizikailag elkülönülő helyen üzemel, és az éles rendszer minden elemét és adatát tartalmazza. Incidens esetén képes átvenni a szervezet éles rendszerének szerepét. Általában a működés a második siteról kicsit lassabb, mert az adatátvitel korlátozottabb, mint a helyben működő infrastruktúraelemek esetében.

6.1.3. Referenciaarchitektúra kis szervezetek számára

Az informatikai infrastruktúra kialakítását alapvetően nemcsak a szervezet mérete, hanem az elvárt rendelkezésre állási szint is meghatározza.

Kis szervezetek esetében az informatikai infrastruktúra kialakítása során az informatikai rendszer elemeit védeni kell a vírusokkal és egyéb kártékony kódokkal szemben, biztonságos internet-hozzáférést kell biztosítani, valamint tűzfalat kell telepíteni, vagy a már meglévőt használni az üzleti rendszer minden elemén. Fontos továbbá, hogy az operációs rendszereket és alkalmazásokat folyamatosan frissíteni kell, illetve mentést kell készíteni a fontos adatokról és információkról. Felügyelni kell a fizikai eszközökhöz és a hálózathoz való fizikai hozzáférést, és biztosítani kell a vezeték nélküli hozzáférési pontok és a hálózat biztonságát. Oktatni kell a munkavállalókat az alapvető biztonsági elvekre; minden munkatársnak önálló, személyre szóló felhasználói fiókkal kell rendelkeznie a szervezet munkaállomásain és az üzleti alkalmazásokban. Ugyanakkor korlátozni kell a munkavállalók hozzáférési jogait az adatokhoz és információkhoz, illetve a szoftverek telepítéséhez.

Mindennek megfelelően egy alapvető architektúra az alábbi elemekből épül fel:



2. ábra

Egy alapvető architektúrát felépítő elemek

Forrás: A szerző saját szerkesztése

A javasolt rendszerelemek az alábbiak.

Tűzfal: a tűzfal a külső támadások ellen védi a szervezet infrastruktúrájának elemeit. Kizárólag azokat a portokat kell megnyitni rajta, melyek a szervezet tevékenységéhez feltétlenül szükségesek. A ma alkalmazott intelligens tűzfalak ezenfelül alapvető vírusvédelmi és IDS/IPS feladatok ellátására is alkalmasak. Amennyiben ezt a funkciót bekapcsolják, a tűzfal figyeli az áthaladó hálózati csomagokat, folyamatosan elemezve azok viselkedését. Az eszköz a tűzfalhasználat, biztonságos internethasználat és a vírus és kártékony szoftverek elleni védelem feladatának ellátásában segít.

Címtár: a felhasználók egyedi azonosításának elősegítésére és a jogainak menedzselésére címtárszerver telepítése javasolt. Ez azonosítja és hitelesíti a szervezet felhasználóit, meghatározva alapvető

jogosultságukat. A címtárszerver segítségével a felhasználók és munkaállomások tevékenysége központilag korlátozható, a biztonsági házirendek ugyaneképp definiálhatók. Az eszköz az egyedi azonosítást és a hozzáférés korlátozást segíti elő.

Fájlszerver/adatbázisszerver: a szerverek a szervezet adatainak tárolására, alkalmazásainak futtatására alkalmasak. Az adatokhoz való hozzáférés a fájl- és adatbázisszervereken fájlokra és rekordokra lebontva korlátozható. Érdemes a felhasználói jogokat szerepkörök alapján meghatározni, megkönnyítve ezzel az adminisztrációs tevékenységeket.

Webszerver: a szervezet a tevékenységével összefüggésben tájékoztatási és kommunikációs céllal működtethet webszervert. Kis szervezeteknél biztonsági célból általában jobb webtárhelyet bérelni, mint saját szervert működtetni.

Levelezőszerver: az eszköz kommunikációs céllal működtethető. A szervezet működtethet saját levelezőszervert, vagy bérelheti szolgáltatásként valamely internet- vagy felhőszolgáltatótól. Amennyiben bérelt levelezési szolgáltatást használ a szervezet, úgy érdemes megfontolni a levelezés titkosítását, a szervezet számára fontos adatok bizalmasságának megőrzése érdekében.

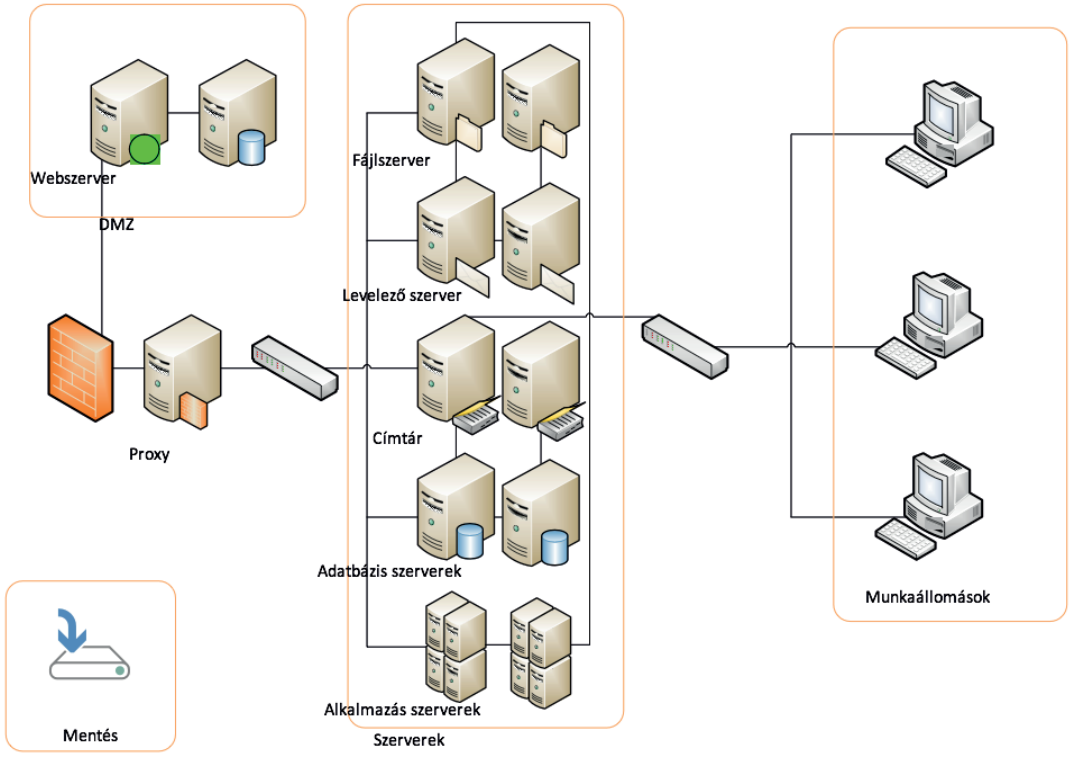
A biztonsági intézkedések megvalósítása során – a hardvertűzfalon kívül – mind a szerver-, mind a kliensgépeken szükség van tűzfalszoftver alkalmazására. A rendszer minden elemére szükséges vírusvédelmet telepíteni. A ma alkalmazott vírusvédelmi megoldások már képesek tűzfalfunkciót is nyújtani, s ezt érdemes is használni. Fontos, hogy a vírusvédelem folyamatosan frissítve legyen, akár kliensenként az internetről, akár központi felügyeleti rendszert használva. Emellett az operációs rendszereket és az alkalmazásokat folyamatosan napra készen kell tartani. Azokat az operációs rendszereket, melyek termékéletciklusuk végén járnak, így nincs rájuk gyártói támogatás, újabb verzióra kell cserélni. Az adatok mentését kis szervezetek esetében az operációs rendszer beépített mentési szolgáltatásával érdemes elvégezni. Természetesen a mentést megelőzően az adatokat osztályozni kell, enélkül nem lehet megállapítani, melyek mentése szükséges a szervezet számára. A fizikai hozzáférés ellenőrzésének leghatékonyabb módja egy beléptető rendszer alkalmazása. Ez lehetővé teszi, hogy az alkalmazottak naplózott módon, akadály nélkül férhessenek hozzá a szervezet azon erőforrásaihoz, melyekhez jogosultságuk van, míg az illetéktelen hozzáférése erősen korlátozva van.

A hálózathoz való hozzáférés korlátozására jól használható eszköz a hálózati aktív eszközökön alkalmazható címszűrés, mely csak azokat az eszközöket engedi be a hálózatba, melyeket már korábban felismert. Kis szervezetek esetében vezeték nélküli hálózati hozzáférés a szervezeti adatok kezelésére nem javasolt. Minden munkavállaló részére saját felhasználói fiókot kell létrehozni minden rendszerhez és alkalmazáshoz, kerülni kell a közös felhasználói fiókok használatát. A munkavállalók részére a felhasználói jogosultságok kiosztásának folyamatát szabályozni kell, definiálva benne, hogy ki a jogosultságok jóváhagyója, illetve hogyan történik a változáskezelés. Fontos szabályozni a jogosultságok visszavonásának folyamatát és felelősségi köreit. Érdemes korlátozni a felhasználók adathordozó-használati és szoftvertelepítési jogait az általuk használt munkaállomásokon. Erre megfelelő eszközt nyújt mind a címtár a központi házirendkezeléssel, mind pedig a vírusvédelmi szoftverek. A rendszer kritikus infrastrukturális elemeiből hideg tartalék tárolása javasolt. Amennyiben ez nem lehetséges, abban az esetben úgy kell méretezni és kialakítani az elemeket, hogy egymás funkcióinak részleges átvételére alkalmasak legyenek (például virtualizációt érdemes használni). A felhasználók biztonságtudatossági képzése rendkívül fontos biztonsági intézkedés a szervezet rendszereinek megfelelő működése szempontjából. Mind a felhasználót azonosító eszközök kezelése, mind pedig a social engineering-en alapuló biztonsági incidensek elkerülése érdekében. Nem szabad megfeledkezni a személyzeti változások kezeléséről az informatikai rendszerben. Az ezzel kapcsolatos változáskezelési folyamat alkalmazható kell legyen. A folyamot a szervezet automatizálhatja.

6.1.4. Referenciaarchitektúra közepes szervezetek számára

A közepes szervezetek informatikai rendszerével kapcsolatos követelményrendszer tartalmazza az előző pontban a kis szervezetekre érvényes követelményeket, de kiegészül néhány további fontos elemmel. Például biztosítani kell a mentések egy példányának külső helyszínen történő tárolását, valamint azt, hogy az internet felől elérhető szolgáltatások demilitarizált zónába kerüljenek. Ki kell alakítani az operációs rendszerek és alkalmazások frissítéséhez a központi frissítésnek és munkaállomásnak a felügyeletrendszerét. Valamint a felhasználói jogosultságok megfelelő korlátozására hálózati leválasztás, szegmentáció bevezetése szükséges.

Ennek megfelelően egy alapvető architektúra az alábbi elemekből épül fel:



3. ábra

A közepes szervezetek számára alapvető architektúrát felépítő elemek

*Forrás:*A szerző saját szerkesztése

A javasolt rendszerelemek az alábbiak.

Tűzfal: a tűzfal a külső támadások ellen védi a szervezet infrastruktúrájának elemeit. Kizárólag azokat a portokat kell megnyitni rajta, melyek a szervezet tevékenységéhez feltétlenül szükségesek. A ma alkalmazott intelligens tűzfalak ezen felül alapvető vírusvédelmi és IDS/IPS feladatok ellátására is alkalmasak. Amennyiben ezt a funkciót bekapcsolják, a tűzfal figyeli az áthaladó hálózati csomagokat, folyamatosan elemezve azok viselkedését. Az eszköz a tűzfalhasználat, a biztonságos internethasználat és a vírus- és kártékony szoftverek elleni védelem feladatának ellátásában segít.

DMZ: a demilitarizált zóna a hálózat egy olyan része, melyet mind az internet irányából, mind pedig a munkahelyi hálózatról csak speciális tűzfalszabályokon keresztül lehet elérni. Általában webszerverek vagy levelezőszerverek levélfogadó (edge trasport) szerepkörű eszközeit helyezik el benne.

Proxy: az internet-hozzáférés biztonságának növelésére, valamint szükség szerint a felhasználói tevékenységek naplózására érdemes a rendszerben proxyt elhelyezni. A naplózási funkción kívül az internetszolgáltatás „gyorsítható" a használatával.

Címtár: a felhasználók egyedi azonosításának elősegítésére és a jogainak menedzselésére címtárszerver telepítése javasolt. Ez azonosítja és hitelesíti a szervezet felhasználóit, meghatározva alapvető jogosultságukat. A címtár segítségével a felhasználók és a munkaállomások tevékenysége központilag korlátozható, a biztonsági házirendek központilag definiálhatók. Az eszköz az egyedi azonosítást és a hozzáférés korlátozást segíti elő.

Fájlszerver/adatbázisszerver: a szerverek a szervezet adatainak tárolására, alkalmazásainak futtatására alkalmasak. Az adatokhoz való hozzáférés a fájl- és adatbázisszervereken fájlokra és rekordokra lebontva korlátozható. Érdemes a felhasználói jogokat szerepkörök alapján meghatározni, megkönnyítve ezzel az adminisztrációs tevékenységeket.

Webszerver: a szervezet a tevékenységével összefüggésben tájékoztatási és kommunikációs céllal működtethet webszervert. Közepes szervezeteknél a webszervert javasolt DMZ-be helyezni, elkerülve ezzel, hogy a webes kérések – ezzel együtt az esetlegesen ezen alapuló támadások – közvetlenül a szervezet rendszerébe kerüljenek.

Levelezőszerver: az eszköz kommunikációs céllal működtethető. A szervezet működtethet saját levelezőszervert, vagy bérelheti szolgáltatásként valamely internet- vagy felhőszolgáltatótól. Amennyiben bérelt levelezési szolgáltatást használ a szervezet, úgy érdemes megfontolni a levelezés titkosítását a szervezet számára fontos adatok bizalmasságának megőrzése érdekében.

Alkalmazásszerverek: az alkalmazásszerverek a szervezet alkalmazásainak kiajánlásán felül központi frissítő és vírusvédelmi szerverként is működhetnek. Közepes szervezeteknél érdemes a munkaállomások központi menedzsmentjére alkalmas alkalmazásokat is használni, melyek segít a szervezetet a működtetései és eszközgazdálkodási feladatok ellátásában.

Naplóelemzés: a különböző szerverek, munkaállomások és hálózati eszközök naplóállományainak központi tárolására, egyszerűbb elemzésére és riportolására központi naplóelemző szerver beállítása javasolt.

Mentés: a rendszerben található kritikus adatokról mentést kell készíteni, melyet lehetőség szerint külső helyszínen kell tárolni. A külső helyszínen tárolt mentések felhasználásával egy incidenst követően a rendszer adatai visszaállíthatók az utolsó mentett állapotra, melyet valószínűleg nem érintett a biztonsági incidens.

Meleg tartalékok: egy közepes szervezetnél mindenképpen szükséges meleg tartalékeszközök alkalmazása. Ez a gyakorlatban annyit jelenti, hogy ez egyes szerverekből nem egy, hanem kettő vagy több példány szolgálja ki a szervezetet. Ebben az esetben nagyrészt terhelésmegosztásban dolgoznak a szerverek, de gyakran előfordul a failover megoldás is.

A biztonsági intézkedések megvalósítása során – a hardvertűzfalon kívül – mind a szerver-, mind a kliensgépeken szükség van tűzfalszoftver alkalmazására. A felhasználók internetes forgalma a beépített proxyszerverrel ellenőrizhető, így detektálható a szokásostól eltérő forgalom. A rendszer minden elemére szükséges a vírusvédelem telepítése. A ma alkalmazott vírusvédelmi megoldások már képesek tűzfalfunkciót is nyújtani, ezeket érdemes használni. Fontos, hogy a vírusvédelem folyamatosan frissítve legyen, akár kliensenként az internetről, akár központi felügyeleti rendszert használva.

Az operációs rendszereket és alkalmazásokat folyamatosan napra készen kell tartani. Azokat az operációs rendszereket, melyek termékéletciklusuk végén járnak, és nincs rájuk gyártói támogatás, újabb verzióra kell cserélni. Az adatok mentését közepes szervezetek esetében az operációs rendszer beépített mentési szolgáltatásával vagy dedikált mentő szoftverrel érdemes elvégezni. Természetesen a mentést megelőzően az adatokat osztályozni kell, enélkül nem lehet megállapítani, melyek mentése szükséges a szervezet számára. A mentéseket másik telephelyen kell tárolni. A fizikai hozzáférés ellenőrzésének leghatékonyabb módja egy beléptető rendszer alkalmazása. Ez lehetővé teszi, hogy az alkalmazottak naplózott módon, akadály nélkül férhessenek hozzá a szervezet azon erőforrásaihoz, melyekhez jogosultságuk van, míg az illetéktelen hozzáférése erősen korlátozva van.

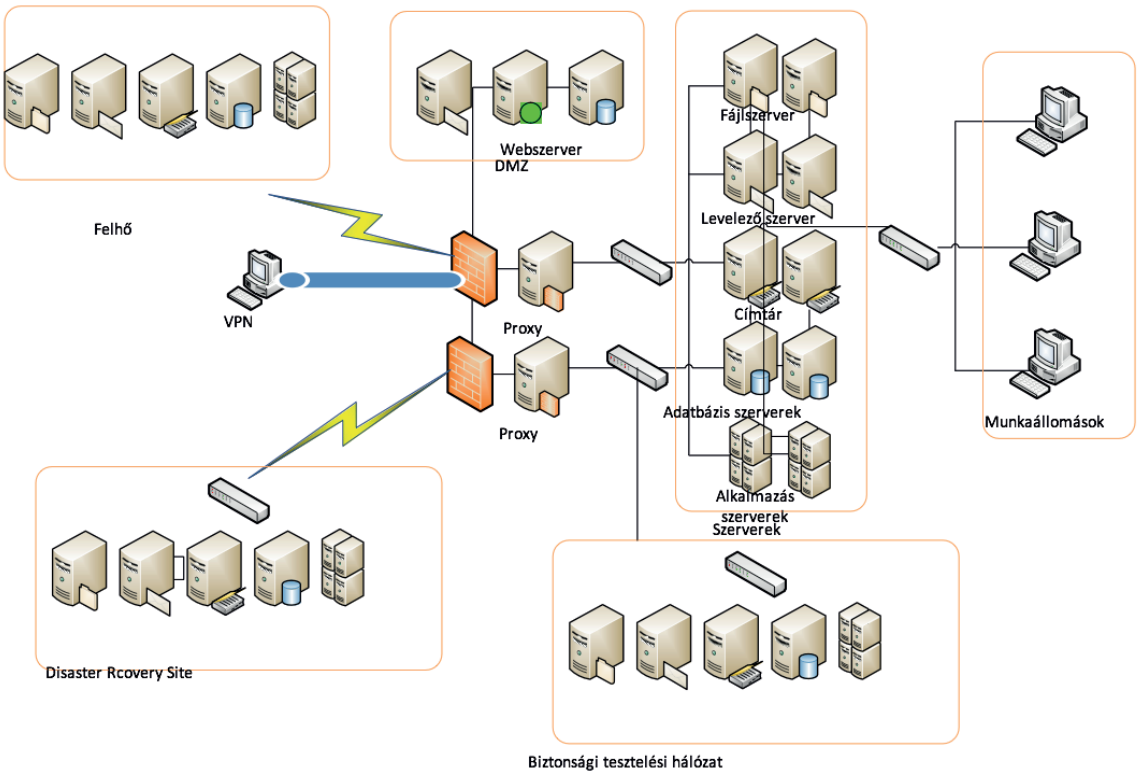
A hálózathoz való hozzáférés korlátozására közepes szervezetek esetében a NAC (Network Access Control) megfelelő szintű védelmet nyújt. Ez a rendszer a hálózathoz kapcsolódni kívánó eszközöket a kapcsolódáskor leellenőrzi, hogy jogosultak-e belépni a hálózatba, illetve hogy az eszközök állapota megfelel-e az elvárásoknak. A közepes szervezetek esetében vezeték nélküli hálózati hozzáférés kialakítása során fontos, hogy az eszközök megfelelő biztonsági beállításokkal legyenek elérhetők. A vezeték nélküli hálózatot javasolt elkülönített hálózati szegmensbe szervezni, mely csak a szükséges mértékben éri el a szervezeti adatokat. Minden munkavállaló részére saját felhasználó fiókot kell létrehozni minden rendszerhez és alkalmazáshoz, kerülni kell a közös felhasználói fiókok használatát. Közepes szervezetek esetében javasolt kétfaktoros hitelesítés használata a felhasználói bejelentkezések során. A munkavállalók részére a felhasználói jogosultságok kiosztásának folyamatát szabályozni kell, definiálva, hogy ki a jogosultságok jóváhagyója, illetve hogyan történik a változáskezelés. Fontos szabályozni a jogosultságok visszavonásának folyamatát és felelősségi köreit. Érdemes korlátozni a felhasználók adathordozó-használati és szoftvertelepítési jogait az általuk használt munkaállomásokon. Erre megfelelő eszközt nyújt mind a központi házirendkezeléssel a címtár, valamint a vírusvédelmi szoftverek. A rendszer kritikus infrastrukturális elemeiből meleg tartalék tárolása javasolt. Az infrastruktúrát úgy kell kialakítani, hogy a különböző szerepköröket két vagy több szerver lássa el, így korlátozottan hibatűrő rendszer alakítható ki (érdemes például virtualizációt használni).

A felhasználók biztonságtudatossági képzése rendkívül fontos biztonsági intézkedés a szervezet rendszereinek megfelelő működése szempontjából, mind a felhasználót azonosító eszközök kezelése, mind pedig a social engineering-en alapuló biztonsági incidensek elkerülése érdekében. Nem szabad megfeledkezni a személyzeti változások kezeléséről az informatikai rendszerben. Az ezzel kapcsolatos változáskezelési folyamat alkalmazható kell legyen. A folyamot a szervezet automatizálhatja.

6.1.5. Referenciaarchitektúra nagy szervezetek számára

A nagy szervezetek informatikai rendszerével kapcsolatos követelményrendszer tartalmazza az előző pontban a közepes szervezetekre érvényes követelményeket, de kiegészül néhány fontos elemmel. Többek között biztosítani kell az informatikai rendszer szerepkör szerinti hálózati szegmentálását, valamint vészhelyzeti tartalékrendszert kell kialakítani, mely az összes létfontosságú rendszerelemet tartalmazza, folyamatosan elérhető és szükség esetén azonnal működésbe állítható. Nagy kiterjedésű rendszerek esetében az adatok folyamatos elérésére felhőszolgáltatások igénybe vétele biztonságos. Biztosítani kell biztonsági tesztelésre alkalmas, elkülönített infrastruktúraelemek elérését.

Ennek megfelelően egy alapvető architektúra az alábbi elemekből épül fel:



4. ábra

A nagy szervezetek számára alapvető architektúrát felépítő elemek

Forrás: A szerző saját szerkesztése

A javasolt rendszer elemek az alábbiak.

Tűzfal: a tűzfal a külső támadások ellen védi a szervezet infrastruktúrájának elemeit. Kizárólag azokat a portokat kell megnyitni rajta, melyek a szervezet tevékenységéhez feltétlenül szükségesek. A ma alkalmazott intelligens tűzfalak ezenfelül alapvető vírusvédelmi és IDS/IPS feladatok ellátására is alkalmasak. Amennyiben ezt a funkciót bekapcsolják, a tűzfal figyeli az áthaladó hálózati csomagokat, folyamatosan elemezve is azok viselkedését. Az eszköz a tűzfalhasználat, a biztonságos internethasználat és a vírus- és kártékony szoftverek elleni védelem feladatának ellátásában segít. Nagy informatikai rendszer esetében legalább két tűzfal használata javasolt két különböző internetszolgáltatótól vásárolt internet-hozzáférés használatával.

DMZ: a demilitarizált zóna a hálózat egy olyan része, mely mind az internet irányából, mind pedig a munkahelyi hálózatról csak speciális tűzfalszabályokon keresztül érhető el. Általában webszerverek vagy levelezőszerverek levélfogadó (edge trasport) szerepkörű eszközeit helyezik el benne.

Proxy: az internet-hozzáférés biztonságának növelésére, valamint szükség szerint a felhasználói tevékenységek naplózására érdemes a rendszerben proxyt elhelyezni. A naplózási funkción kívül az internetszolgáltatás „gyorsítható” a használatával.

Címtár: a felhasználók egyedi azonosításának elősegítésére és a jogaik menedzselésére címtárszerver telepítése javasolt. Ez azonosítja és hitelesíti a szervezet felhasználóit, meghatározva alapvető

jogosultságukat. A címtárszerver segítségével a felhasználók és a munkaállomások tevékenysége központilag korlátozható, a biztonsági házirendek központilag definiálhatók. Az eszköz az egyedi azonosítást és a hozzáférés korlátozást segíti elő.

Fájlszerver/adatbázisszerver: a szerverek a szervezet adatainak tárolására, alkalmazásainak futtatására alkalmasak. Az adatokhoz való hozzáférés a fájl- és adatbázisszervereken fájlokra és rekordokra lebontva korlátozható. Érdemes a felhasználói jogokat szerepkörök alapján meghatározni, megkönnyítve ezzel az adminisztrációs tevékenységeket.

Webszerver: a szervezet a tevékenységével összefüggésben tájékoztatási és kommunikációs céllal működtethet webszervert. Közepes szervezeteknél a webszervert javasolt DMZ-be helyezni, elkerülve ezzel, hogy a webes kérések – így az esetlegesen ezeken alapuló támadások – közvetlenül a szervezet rendszerébe kerüljenek.

Levelezőszerver: az eszköz kommunikációs céllal működtethető. A szervezet működtethet saját levelezőszervert, vagy bérelheti szolgáltatásként valamely internetszolgáltatótól vagy a Microsofttól. Amennyiben bérelt levelezési szolgáltatást használ a szervezet úgy érdemes megfontolni a levelezés titkosítását a szervezet számára fontos adatok bizalmasságának megőrzése érdekében.

Alkalmazásszerverek: ezek a szervezet alkalmazásainak kiajánlásán felül központi frissítő és vírusvédelmi szerverként is működhetnek. Közepes szervezeteknél érdemes a munkaállomások központi menedzsmentjére alkalmas alkalmazásokat is használni, melyek segítenek a működtetési és eszközgazdálkodási feladatok ellátásában.

Meleg tartalékok: egy közepes szervezetnél mindenképpen szükséges meleg tartalékeszközök alkalmazása. Ez a gyakorlatban annyit jelenti, hogy ez egyes szerverekből nem egy, hanem kettő vagy több példány szolgálja ki a szervezetet. Ebben az esetben nagyrészt terhelésmegosztásban dolgoznak a szerverek, de gyakran előfordul a failover megoldás is.

Hálózati szeparáció: nagy rendszerek esetében a hálózat eltérő funkciójú szegmenseit különböző alhálózatokba kell szervezni. Ennek megfelelően külön alhálózatot kaphatnak a munkaállomások, a szerverek, a tesztrendszerek, a menedzsment rendszere, illetve a biztonsági tesztelésre alkalmazott rendszer. Hálózati szeparáció használatával egyszerűen menedzselhető a munkaállomások hozzáférési joga a különböző alhálózatokban található szolgáltatásokhoz.

Biztonsági tesztelési rendszer: a rendszer a szervezet minden infrastruktúraeleméből és alkalmazásából tartalmaz egy példányt, melyen a frissítéseket és az új biztonsági beállításokat tesztelik. Ezzel a módszerrel elkerülhető, hogy a frissítések vagy biztonsági beállításváltozások üzemkiesését okozzanak az éles rendszerben.

Vészhelyzeti tartalékrendszer: a szervezet rendszereinek olyan leképezése, mely egy esetleges incidenst követően képes átvenni az éles rendszer funkcióit. Fontos, hogy a vészhelyzeti tartalékrendszerek adattartalma megegyezzen az éles rendszerével, a folyamatos adatszinkronizálást meg kell oldani.

Felhő: nagy szervezetek gyakran használják szolgáltatásaik egy részének futtatására. A felhőben lehetőség van a szervezet bármely szolgáltatásának kialakítására, az adatok tárolására, valamint akár vészhelyzeti tartalékrendszer kialakítására úgy, hogy a virtuális infrastruktúraelemek a szervezet felügyelete alatt vannak.

VPN: nagy szervezetek esetében mindennapos, hogy a munkatársak VPN kapcsolaton keresztül érik a szervezet belső erőforrásait. Ilyenkor a felhasználói munkaállomás és a szervezet rendszerei között egy titkosított kommunikációs csatorna jön létre.

A biztonsági intézkedések megvalósítása során – a hardvertűzfalon kívül – mind a szerver-, mind a kliensgépeken szükség van tűzfalszoftver alkalmazására. A felhasználók internetes forgalma a beépített proxyval ellenőrizhető , melynek segítségével detektálható a szokásostól eltérő forgalom is. A rendszer minden elemére szükséges vírusvédelem telepítése. A ma alkalmazott vírusvédelmi megoldások már képesek tűzfalfunkciót is nyújtani, így érdemes ezeket használni. Fontos, hogy a vírusvédelem folyamatosan frissítve legyen, akár kliensenként az internetről, akár központi felügyeleti rendszert használva. Emelett az operációs rendszereket és alkalmazásokat is folyamatosan napra készen kell tartani. Azokat az operációs rendszereket, melyek termékéletciklusuk végén járnak, és nincs rájuk gyártói támogatás, újabb verzióra kell cserélni. Az adatok mentését nagy szervezetek esetében az operációs rendszer beépített mentési szolgáltatásával vagy dedikált mentőszoftverrel érdemes elvégezni. Természetesen a mentést megelőzően az adatokat osztályozni kell, enélkül nem lehet megállapítani, melyek mentése szükséges a szervezet számára. A mentéseket másik telephelyen kell tárolni. A fizikai hozzáférés ellenőrzésének leghatékonyabb módja egy beléptető rendszer alkalmazása. Ez lehetővé teszi, hogy az alkalmazottak naplózott módon, akadály nélkül férhessenek hozzá a szervezet azon erőforrásaihoz, melyekhez jogosultságuk van, míg az illetéktelen hozzáférés erősen korlátozva van.

A hálózathoz való hozzáférés korlátozására nagy szervezetek esetében a NAC (Network Access Control) nyújt megfelelő szintű védelmet. Ez a rendszer a hálózathoz kapcsolódni kívánó eszközöket a kapcsolódáskor leellenőrzi, hogy jogosultak-e belépni a hálózatba, illetve hogy az eszközök állapota megfelel-e az elvárásoknak. Nagy szervezetek esetében vezeték nélküli hálózati hozzáférés kialakítása során fontos, hogy az eszközök megfelelő biztonsági beállításokkal legyenek elérhetők. A vezeték nélküli hálózatot minden esetben elkülönített hálózati szegmensbe kell szervezni, mely csak a szükséges mértékben éri el a szervezeti adatokat. Minden munkavállaló részére saját felhasználói fiókot kell létrehozni minden rendszerhez és alkalmazáshoz, kerülni kell a közös felhasználói fiókok használatát. Nagy szervezetek esetében ajánlott a hitelesítés során kétfaktoros eljárást alkalmazni. Bizonyos szerepkörök esetében – rendszeradminisztrátor, fejlesztők stb. – a kétfaktoros hitelesítés nem ajánlás, hanem előírás. A munkavállalók részére a felhasználói jogosultságok kiosztásának folyamatát szabályozni kell, definiálva, hogy ki a jogosultságok jóváhagyója, illetve hogyan történik a változáskezelés. Fontos szabályozni a jogosultságok visszavonásának folyamatát és felelősségi köreit. Korlátozni kell a felhasználók adathordozó-használati és szoftvertelepítési jogait az általuk használt munkaállomásokon. Erre megfelelő a központi házirendkezeléssel a címtár, valamint a vírusvédelmi szoftverek. A rendszer kritikus infrastrukturális elemeiből meleg tartalék tárolása javasolt. Az infrastruktúrát úgy kell kialakítani, hogy a különböző szerepköröket két vagy több szerver lássa el, így korlátozottan hibatűrő rendszer alakítható ki (érdemes például virtualizációt használni).

A felhasználók biztonságtudatossági képzése rendkívül fontos biztonsági intézkedés a szervezet rendszereinek megfelelő működése szempontjából, mind a felhasználót azonosító eszközök kezelése, mind pedig a social engineering-en alapuló biztonsági incidensek elkerülése érdekében. Szükség van olyan vészhelyzeti tartalékrendszer kialakítására, mely az éles rendszer esetleges leállása esetén képes a szervezet folyamatos kiszolgálására az éles rendszer újraindulásáig. Ez akár felhőszolgáltató rendszerben is kialakítható. A szervezet rendszereit egymástól elkülönített hálózati szegmensekbe kell szervezni, melyek kommunikációja hálózati szabályokkal korlátozható. Szükséges olyan biztonsági tesztelési rendszer kialakítása, mely lehetőséget nyújt a frissítések és beállítások kitesztelésére az élessel megegyező rendszeren. A VPN csatormát megfelelő módon kell titkosítani, illetve a felhasználók részére a szervezeti erőforrások használatához és a VPN-hez mindenképpen kétfaktoros hitelesítést kell előírni. Nem szabad megfeledkezni a személyzeti változások kezeléséről az informatikai rendszerben. Az ezzel kapcsolatos változáskezelési folyamat alkalmazható kell legyen. Nagy szervezetek esetén érdemes a változáskezelési folyamatot automatizálni.

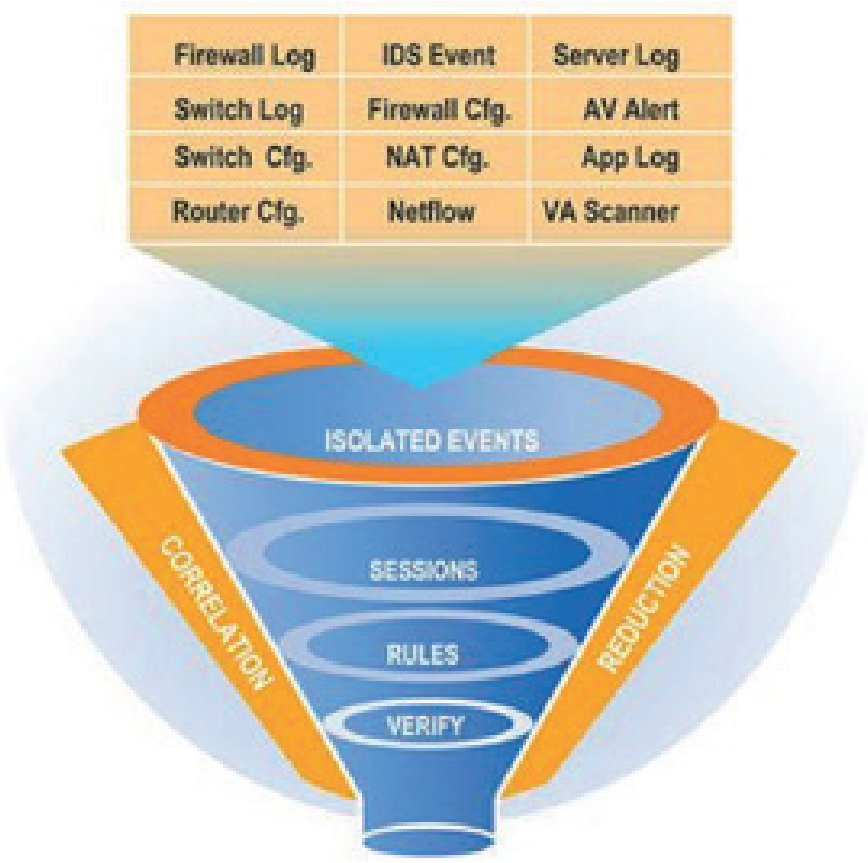
6.1.6. SIEM, Cyber Threat Intelligence, SOC

A SIEM a Security Information and Event Management rövidítése. Ebben a megoldásban egyesül a biztonsági információ felügyelet (SIM – Security Information Management) és a biztonsági eseménykezelés (SEM – Security Event Management).

A SIEM rendszerek célja, hogy átfogó képet adjanak egy szervezet biztonsági állapotáról és a benne folyó tevékenységekről.

Alapelve egyszerű: a hagyományos naplógyűjtésen túl (melyben az egyes hálózati elemek, operációs rendszerek és alkalmazások naplóállományait egy központi naplószerverre gyűjtjük), nem pusztán tárolja az összegyűjtött naplóállományokat, hanem korrelálja és normalizálja azokat, és különféle egyéb elemzéseket is végez rajtuk.

Az így keletkezett eredmények maguk az események, melyekről a rendszer el tudja dönteni, hogy azok valójában biztonsági események-e, és ha igen, milyen súlyosságúak, és/vagy üzemeltetési eseményekről van-e inkább szó, amelyek nem biztonsági, de üzemetetési szempontból ugyancsak értékes információkat tartalmazhatnak.



5. ábra

A SIEM rendszer működése

Forrás: https://techstory.in/security-operations-center

A biztonsági események felfedezése kulcsfontosságú, és diszkrét naplóállományokból gyakran lehetetlen egy összetett támadást észlelni. Mivel a jelenlegi támadások egyre bonyolultabbak, a SIEM rendszereknek egyre nagyobb szerepük van egy nagy és összetett infrastruktúrával rendelkező szervezet biztonsági gyakorlatában.

A SIEM által felfedezett és rangsorolt biztonsági eseményekhez különféle risztások kapcsolhatók. Extrém esetben a SIEM automatikusan be is tud avatkozni, amennyiben olyan kritikus biztonsági eseményről van szó, amely ezt indokolja. További funkciója lehet a SIEM rendszernek, hogy ha

nem is avatkozik be automatikusan az adott biztonsági esemény megszűntetésébe, de javaslatot tehet a rendszerek üzemeltetőinek, miként kerülhetnek el a jövőben egy a felfedezetthez hasonló biztonsági eseményt.

A SIEM rendszerek a legfontosabb építőelemei a korszerű Security Operation Center-nek (röviden SOC).

6. ábra

A SOC építőelemei

Forrás: www.solutions-numeriques.com

A SOC olyan, 24 órában működtetett biztonsági központ, ahol az adott szervezeten belül fellépő biztonsági eseményeket technikai szinten monitorozzák és kezelik. A 6. ábrán jól láthatjuk, hogy egy ilyen központnak az egyik legfontosabb bemeneti információforrása maga a SIEM rendszer által publikált és rangsorolt biztonsági esemény.

Ugyancsak fontos bemeneti információ az úgynevezett Cyber Threat Intelligence (CTI). A CTI olyan, a kibertér fenyegetettségére vonatkozó információkat tartalmaz, amelyeknek a a SOC-ba való becsatornázása után az üzemeltetők célirányosan és hatékonyabban tudnak fellépni a veszélyekkel szemben. Ilyen információk lehetnek taktikai (támadási módszertanok, eszközök stb.), technikai (milyen károkozók fertőznek), üzemeltetési (konkrét támadások részletei) vagy stratégiai (kockázati értékelések, döntéshez szükséges információk) jellegűek. A CTI-ket erre specializált biztonsági

szolgáltatóktól lehet beszerezni, melyek leggyakrabban valamely vezető kiberbiztonsági gyártóhoz köthetők. Vannak ingyenes és fizetős CTI szolgáltatások, és lehet geográfiai vagy akár technológiai területre szűkített CTI-t is igénybe venni.

6.1.7. Magyarországon elérhető biztonsági gyártók, megoldásaik és kiválasztásuk

Magyarországon lényegében az összes fejlett biztonsági gyártó megoldása szabadon elérhető. A legtöbbjüknek saját irodája és kereskedelmi hálózata is működik, melyektől mind kereskedelmi, mind pedig műszaki segítséget és támogatást kaphatunk.

Az egyes feladatokra vonatkozóan a kiválasztás szempontjai több rétegűek lehetnek. Figyelembe veendők a műszaki alkalmassági szempontok, a gazdasági szempontok és a közbeszerzési szempontok.

6.1.7.1. Műszaki alkalmassági szempontok

Műszaki szempontból többféleképpen közelíthetjük meg a kérdést. Talán a legpraktikusabb, ha fel tudunk állítani egy olyan funkciórendszert, mely világossá teszi, mit várunk az adott megoldástól. Ehhez részletesen ismernünk kell a piacon elérhető fejlett megoldások paramétereit, és azt, hogy mit is várhatunk el ma egy korszerű terméktől.

Tovább lehet szűkíteni a kört, ha megvizsgáljuk a különféle piackutató és tesztcégek egyes termékkörre vonatkozó vizsgálatait. Ez több mindenben segíthet. Egyrészt iránymutatást adhat arra nézve, amit az előzőekben részleteztünk, miszerint mit is várhatunk egy mai korszerű terméktől az adott feladatban. A másik segítség, hogy jellemzően osztályozza a termékeket műszaki és/vagy gazdasági szempontok alapján, és segít szűkíteni a kört az általuk ajánlott és/vagy piacvezető gyártókra vagy termékekre.

A legismertebb ilyen tesztek a Gartner, a IDC és az NSS Lab vizsgálatai.

A Gartner több területen végez vizsgálatokat és mindegyikről készít egy Magic Quadrant nevű infografikát. Ebben a mátrixban, az egyik tengelyek helyezi el az adott termékkörre vonatkozó gyártókat aszerint, hogy milyen érettségű, mennyire fejlett a technológiai víziója a termékkörre vonatkozóan. A másik tengelyen azt ábrázolják, hogy mennyire tudja a vízióit megvalósítani. Ez alapján a jobb felső negyedbe kerülnek a vezető gyártók (Leaders), akik az adott termékkörben a Gartner szerint piacvezetőnek számítanak.

Az IDC minden évben elkészíti az IT biztonsággal kapcsolatos felmérését/piackutatását, és ezen belül eladási statisztikák alapján rangsorolja az egyes gyártókat. Ez is orientációt nyújthat arra vonatkozóan, melyik gyártók a legnépszerűbbek az adott területen. (Például az első 5 helyezettre szűkítve a kiválasztást túlságosan nem nyúlhatunk mellé.)

Az NSS Lab egy technológiai teszteket és gazdasági szempontokat ötvöző szervezet. Több biztonsági területen végez egyértelmű műszaki teszteket, melyek körülményeit, a labor felépítését és a többi paramétert nyilvánosságra hozzák, így bárki reprodukálhatja az általuk készített teszteket. Ez minden szempontból komoly hitelt és megbízhatóságot garantál az így nyilvánosságra hozott eredményeknek. Ezenkívül a rangsorolásuk során figyelembe vesznek gazdasági szempontokat, vagyis azt, hogy mennyibe kerül egy adott adatmennyiség védelme a különféle gyártók azonos funkciójú termékével megoldva. Az eredményeket szintén egy infografikán ábrázolják, ahol az egyik tengelyen a biztonsági hatékonyság, a másikon pedig az egységnyi adamennyiség védelmi költsége található. Az általuk ajánlott (recommended) kategóriába sorolt termékek nemcsak műszakilag felelnek meg az adott feladatnak, hanem ár/érték arányukat tekintve is a legkedvezőbbek a piacon.

A kiválasztás során figyelembe vehetjük egy vagy több piackutató és tesztcég ajánlását is, attól függően, hogy az adott termékkör, amit be kívánunk szerezni, mennyire összetett vagy mennyire számít kiforrott, érett technológiának.

6.1.7.2. Gazdasági szempontok

A kiválasztás gazdasági szempontjai összetettek. Közgazdasági szempontból leginkább úgynevezett TCO (Total Cost of Ownership, Teljes Bekerülési Érték) adatokat számítanak, és ezeket hasonlítják össze.

A TCO számításban adott időszakra vetítve (ez jellemzően lehet, 1, 3 és 5 év) figyelembe veszik az összes, az adott termékre vonatkozó költséget. Ebbe beleszámítanak az úgynevezett beszerzési (Capex) és a működési költségek (Opex).

A beszerzési költségek a hardvertermék ára vagy a szoftvertermék egyszeri licenszdíja, amennyiben öröklicenszről (perpetual license) van szó. Ha nem erről, hanem évente megújítandó licenszről van szó, akkor az éves licenszdíj annyiszor számít bele a TCO-ba, ahány évre kalkuláljuk azt.

A működési költségek kalkulálása bonyolultabb. A legtöbb IT biztonsági megoldáshoz tartozik egy úgynevezett éves frissítési díj, amely jellemzően két részből áll. Egyszer az adott termék gyártói és/vagy megoldásszállítói éves műszaki támogatásának díja, másrészt – bizonyos termékek (például antivírus, IDS/IPS) esetében – az úgynevezett mintaadatbázis éves frissítésének a díja. Értelemszerűen ez a költség is annyiszor számít bele a TCO-ba, ahány évre számítjuk azt.

A működési költségekbe beleszámít továbbá minden egyéb, az adott rendszer működtetéséhez szükséges költség. Például, ha ki kell képezni a kollégákat az új rendszer üzemeltetésére, akkor a tanfolyam díja vagy az üzemeltetést végző belső kollégák bérköltsége (mert az egyes termékek eltérő kvalitású kollégákat igényelhetnek az üzemeltetésre, és akár eltérő időráfordítással is üzemeltethetők a különféle termékek). További költség lehet, ha az üzemeltetést kiszervezzük. Ebben az esetben a kiszervezés adott időszakra vonatkozó költsége is számítandó.

A különböző gyártók termékeinek/megoldásainak ugyanazon időszakra kiszámított TCO értékei összehasonlíthatók, és a műszaki szempontok kombinációival optimális megoldás választható.

6.1.7.3. Közbeszerzési szempontok

Az állam- és közigazgatási szervek beszerzéseire külön szabályok vonatkoznak. Ez a Közbeszerzési törvény, ami részletesen taglalja, hogy az egyes szervezetek milyen eljárásrendek keretén belül szerezhetnek be adott termékeket.

A közbeszerzés rendszerén belül megkülönböztetjük a *központosított közbeszerzést.* Vannak olyan szervezetek, akik kötelezően részt kell, hogy vegyenek a központosított közbeszerzés rendszerében, és vannak önként csatlakozó szervezetek. A logika a központosított közbeszezés mögött az, hogy egy központi beszerző szervezet, jelen esetben a Közbeszerzési és Ellátási Főigazgatóság (KEF) egy előzetes minősítő eljárást folytat le, melynek keretein belül mind műszakilag, mind gazdaságilag megszűrik mind a beszállítókat, mind pedig az adott termékköre vonatkozó, elérhető termékeket. Az intézmények innentől kezdve egy szűrt listából választhatnak.

A központosított közbeszerzés rendszere úgynevezett kiemelt termékekre vonatkozik. Azok az intézmények, akik kötelezően vagy önkéntesen csatlakoztak a központosított közbeszerzés rendszeréhez, a kiemelt termékek körébe esőket kötelezően a központosított közbeszerzés keretein belül kötelesek beszerezni. Ettől csak kivételes esetekben térhetnek el, melyeket kormányrendelet szabályoz.

Az informatikai eszközök, számítógépek, szoftverek, nyomtatók, hálózati elemek és IT biztonsági termékek a kiemelt termékek körébe tartoznak, ezért azon intézmények, akikre kötelezően vonatkozik a központosított közbeszerzés rendszere (vagy önkéntesen csatlakoztak hozzá) ilyen megoldásokat ezen metódus szerint szerezhetnek be, és így csak azokat, melyek megfeleltek a KEF előzetes eljárási feltételeinek, és csak azoktól a cégektől szerezhetnek be, akik szintén megfeleltek ezen követelményeknek. Az ettől való eltérést egy közbeszerzési szakértő tudja megvizsgálni, és tanácsot adni.

6.1.8. Megfelelés az Ibtv. követelményeinek

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény és a végrehajtására kiadott 41/2015. (VII. 15.) BM rendelet alapvetően a NIST által publikált kontrolljegyzék alapján került kialakításra.

A jogszabály és a vonatkozó végrehajtási rendelet elkészítésekor a jogalkotó figyelembe vette a nemzetközi ajánlásokat, ennek megfelelően a vonatkozó szabályokat alapvetően a NIST által tett ajánlások figyelembe vételével fogalmazta meg.

A jogalkotó jogszabályban a hatálya alá tartozó szervezetek részére előír olyan szabályokat és tevékenységeket, melyek elvégzése a jogszabályi előíráson túl megfelel a NIST keretrendszernek és ajánlásainak, valamint az azokban foglalt biztonsági kontrollok alkalmazásához is elengedhetetlen. Ezek a tevékenységek az alábbiak:

- a szervezet aktuális biztonsági szintjének meghatározása;
- a szervezet információbiztonsági céljának megfogalmazása, a szükséges elérendő biztonsági szint meghatározása;
- a biztonsági cél eléréséhez szükséges lépések meghatározása;
- megfelelő kommunikáció a külső és belső érdekeltek között.

Az Ibtv. alapvetően a NIST ajánlásait követi, bár a rendszerek biztonsági besorolása során az ajánlás által javasolt háromszintű biztonsági besorolás helyett öt szintet definiál. A biztonsági szintek pontos definíciója a végrehajtási rendeletben megtalálható, melyből az alábbi idézetek is származnak. [1]

„Az érintett szervezet biztonsági szintje 1., ha a szervezet nem üzemeltet és nem fejleszt elektronikus információs rendszert, és saját hatáskörben erre más szervezetet vagy szolgáltatót sem vesz igénybe. Az adatfeldolgozás módját nem maga határozza meg, az adatkezelés tekintetében technikai vagy információtechnológiai döntést nem hoz, a használt elektronikus információs infrastruktúra kialakítása tekintetében döntési jogköre – ide nem értve a szervezet munkavégzését érintő informatikai rendszerelemek elhelyezését – nincs, egyedi adatokat és információkat kezel vagy dolgoz fel, és kritikus adatot nem kezel. A szervezet információbiztonsági tevékenysége elsődlegesen az elektronikus információs rendszerrel kapcsolatba kerülő személyek információbiztonsággal kapcsolatos kötelezettségeinek szabályozására, számonkérésére terjed ki, addig a mértékig, ameddig a szervezet vagy az egyes személyek tevékenysége az elektronikus információs rendszerre hatást tud gyakorolni.”

„Az érintett szervezet biztonsági szintje 2., ha a szervezet vagy szervezeti egység az 1. szinthez rendelt jellemzőkön túl olyan elektronikus információs rendszert használ, amely személyes adatokat kezel, és a szervezet jogszabály alapján kijelölt szolgáltatót vesz igénybe.”

„Az érintett szervezet biztonsági szintje 3., ha a szervezet vagy szervezeti egység a 2. szinthez rendelt jellemzőkön túl szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti azt. A szervezet kritikus adatot, nem minősített, de nem közérdekű, vagy közérdekből nyilvános adatot kezel, központi üzemeltetésű, és több szervezetre érvényes biztonsági megoldásokkal védett elektronikus információs rendszerek vagy zárt célú elektronikus információs rendszer felhasználója, illetve feladatai támogatására más külső szolgáltatót vesz igénybe.”

„Az érintett szervezet biztonsági szintje 4., ha a szervezet vagy szervezeti egység a 3. szinthez rendelt jellemzőkön túl elektronikus információs rendszert vagy zárt célú elektronikus információs rendszert üzemeltet vagy fejleszt.”

„Az érintett szervezet biztonsági szintje 5., ha a szervezet vagy szervezeti egység a 4. szinthez rendelt jellemzőkön túl európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek elektronikus információs rendszereinek üzemeltetője, fejlesztője, illetve az információbiztonsági ellenőrzések, tesztelések végrehajtására jogosult szervezet vagy szervezeti egység.”

---

[1] Az Ibtv. végrehajtási rendelete, második melléklet. Elérhető: http://lbtv.hu/ibtv/vegrehajtasi-rendelet (a letöltés ideje: 2017. április 20.)

A NIST besorolásai az alábbiak:

Low: A bizalmasság sértetlenségének és a rendelkezésre állásnak a várható vesztesége negatív hatással van a szervezet működésére, a szervezeti eszközök elérésére, valamint az ott dolgozókra.

Moderate: A bizalmasság sértetlenségének és a rendelkezésre állásnak a várható vesztesége súlyosan káros hatással van a szervezet működésére, a szervezeti eszközök elérésére, valamint az ott dolgozókra.

High: A bizalmasság sértetlenség és rendelkezésre állás várható vesztesége súlyos vagy végzetesen káros hatással van a szervezet működésére, a szervezeti eszközök elérésére, valamint az itt dolgozókra.

Az Ibtv. biztonsági szintjei a NIST ajánlását finomhangolják, de alapvetően megfeleltethetők annak.

2. táblázat

Az Ibtv. és a NIST szintjeinek megfeleltethetősége

Ibtv szintjei	NIST szintjei
1. szint	Low
2. szint	Low
3. szint	Moderate
4. szint	Moderate
5. szint	High

Forrás: A szerző saját szerkesztése

Az Ibtv.-ben az elektronikus információs rendszerekkel kapcsolatosan előírt biztonsági intézkedések hűen követik a korábbi részekben tárgyalt eseménykezelési lépéseket. Az *adatok és rendszerek osztályba sorolás*ának*, a kockázatelemzés* elvégzésének követelménye teljes egészében megfelel a NIST által javasolt Identify fázisnak, ahol a szervezeti biztonsági környezet, a kezelt adatok szintje és az üzleti környezet kerül meghatározásra.

A *megelőzés és a korai figyelmeztetés* fázisban a szervezetek olyan biztonsági eszközöket és folyamatokat működtetnek, melyek segítséget nyújtanak az elektronikus információs rendszer védelmében az esetleges fenyegetésekkel szemben. Ez a lépés a NIST által javasolt Protect fázisnak feleltethető meg, melyben a rendszerek védelmére alkalmazott eljárások és eszközök összegyűjtése a meghatározott feladat.

Az észlelés azon képességek, technikák és folyamatok alkalmazását jelenti, melyek segítségével a szervezet képes az esetleges incidensek felfedezésére. A NIST által javasolt Detect fázis ugyanezt a célt szolgálja.

A *reagálás* a bekövetkezett eseményre való válaszlépések és folyamatok összessége; megfelelően a NIST által javasolt Respond lépésben foglaltaknak.

A *biztonsági események kezelése* keretében az elektronikus információs rendszerek normál működésének visszaállítása, a tanulságok beépítése a gyakorlatba, illetve a megfelelő kommunikáció történik, és az együttműködés az érintett szervezetekkel; összhangban a NIST által javasolt Recover lépéssel.

A végrehajtási rendeletben kifejtett, az állami és önkormányzati szervezetek biztonsági szintbe sorolásához irányadó 3. számú melléklet tartalma jól megfeleltethető a NIST 800-53 ajánlatban definiált kontrolloknak. A szervezet besorolási szintjét tulajdonképpen az ezeknek a kontrolloknak való megfelelés szintje határozza meg.

A jogszabályok megfelelése a vonatkozó, nemzetközileg elfogadott és alkalmazott ajánlásoknak az incidenskezelés eszköztárának az egységesítését, a nemzetközi kapcsolattartás és az érintettek közötti kommunikáció megkönnyítését szolgálja.

A fentiekben ismertetett, az incidensmenedzsmentben alkalmazott eszközök, illetve a javasolt referenciaarchitektúrák a NIST követelmények alapján kerültek meghatározásra. Ennek megfelelően a javasolt eszközök és rendszerek mind az Ibtv. hatálya alá tartozó, mind pedig a gazdálkodási szervezeteknél alkalmazhatók.

6.1.9. Összefoglaló

A témakör végére érve látható, hogy a szerveztek informatikai rendszereinek biztonsági megközelítése nélkülözhetetlen napjainkban. Az elektronikus információrendszerek, valamint az elektronikus ügyintézés lehetőségének egyre szélesebb körű elterjedésével adataink egyre nagyobb veszélynek vannak kitéve. A fejezettel betekintést kívántunk nyújtani a szervezetek incidenskezelési gyakorlatába és az ennek során alkalmazott műszaki eszközök körébe.

A téma keretében a hallgató megismerkedhetett az incidenskezelés fontosabb lépéseivel, valamint az azokat szabályozó ajánlásokkal.

Részletesen bemutattuk az incidenskezelés egyes lépései során végrehajtandó feladatokat, illetve a szervezeteknél előforduló, az elektronikus információs rendszernek a feladatokkal kapcsolatos lehetséges paramétereit. Ezek a tulajdonságok jól jelzik az érintett szervezet informatikai érettségét.

Bemutattuk a különböző méretű szervezeteknél javasolt informatikai architektúrákat is. Ezeknél minden esetben tárgyaltuk a szervezet informatikai rendszerével szemben támasztott követelményeket, valamint az ezeknek való megfelelés biztosításának módjait, feltételeit.

Az utolsó részben a szabályozási környezetet vizsgáltuk, kiemelve a hazai és a nemzetközi szabályozás közti eltéréseket.

Felhasznált irodalom

MITNICK, Kevin D. – SIMON, William L. (2003): *A legendás hacker – A megtévesztés művészete*. Budapest, Perfacto-Pro Kft.

MITNICK, Kevin D. – SIMON, William L. (2006): *A legendás hacker 2. – A behatolás művészete*. Budapest, Perfacto-Pro Kft.

DÓSA Imre – HARSÁN Péter – HORVÁTH Zsolt – KESSELYÁK Péter – KÖDMÖN István – MÓRICZ Pál – TARJÁN Gábor (2008): *Hétpecsétes történetek – Információbiztonság az ISO 27001 tükrében.* Budapest, Hétpecsét Információbiztonsági Egyesület.

CSEH Zsolt – DÓSA Imre – KESSELYÁK Péter – KÖDMÖN István – MOLNÁR László – MÓRICZ Pál – NAGY Péter – REDLER Sándor – TARJÁN Gábor (2014): Hétpecsétes történetek II. – *Információbiztonság az ISO 27001 tükrében.* Budapest, Hétpecsét Információbiztonsági Egyesület.

VISNYEI Aladár – VÖRÖS Gábor (é. n.): *A számítógépes információbiztonság alapjai*. Budapest, LSI Oktatóközpont.

KÜRTI Sándor – FABIÁNYI Gábor (2008): *20 éves a KÜRT, az Infostrázsa – Információbiztonság és egyéb pikáns ügyek*. Budapest, Kürt Rt.

HORVÁTH Gergely Krisztián (2013): *Közérthetően nem csak az IT biztonságról – Információ és IT biztonsági kultúra fejlesztése a közigazgatásban*. Budapest, KIFÜ. Elérhető: http://kifu.gov.hu/kifu/sites/default/files/IT_brosura_v7.pdf (a letöltés ideje: 2017. április 20.)

NIST (2014): *Cybersecurity Framework*. Elérhető: www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (a letöltés dátuma: 2017. április 20.)

SCHUBERT Tamás (é. n.): *Hálózati szolgáltatások tervezése és működtetése.* Tantárgyleírás. Óbudai Egyetem, Neumann János Informatikai Kar. Elérhető: http://users.nik.uni-obuda.hu/to/tanterv/kovetelmenyek/907/halozati-szolgaltatasok-tervezese-es-mukodtetese (a letöltés ideje: 2017. április 20.)

JAMIL, Amir (2010). *The difference between SEM, SIM and SIEM.* Elérhető: www.gmdit.com/NewsView.aspx?ID=9IfB2Axzeew= (a letöltés ideje: 2017. április 20.)

SWIFT, David (2006). *A Practical Application of SIM/SEM/SIEM, Automating Threat Identification.* Elérhető: www.sans.org/reading-room/whitepapers/logging/practical-application-sim-sem-siem-automating-threat-identification-1781 (a letöltés ideje: 2017. április 20.)

7. A SZERVEZETEN BELÜLI INCIDENSKEZELÉSI GYAKORLATOK SZERVEZÉSE

Solymos Ákos – CISM – CRISC

7.1. Végfelhasználói feladatok az incidenskezelésben

Az incidenskezelésnek, de legfőképp egy potenciális incidens felismerésének egyik legfontosabb kulcsszereplője a végfelhasználó. Az ő tudásán, kockázatérzékenységén és biztonságtudatosságán múlik sok esetben egy-egy támadás sikeres lefutása vagy éppen felismerése és megszakítása. Számos példát láthatunk arra mind a közel, mind a kicsit távolabbi múltból, hogy a felhasználók nem megfelelően képzettsége miatt percek és/vagy órák alatt az egész világon végigrobogó vírustámadások, vagy egy-egy cég életét jelentősen befolyásoló támadások valósulhatnak meg.

Első esetre a legjobb példa a LOVELETTER, vagy ILOVEYOU vírus néven elhíresült féreg. Ez 2000. május 4-én indult világhódító útjára, hogy pár nap alatt beírja magát a világ információvédelmi történelemkönyvébe, ahol ékes példaként szolgál a végfelhasználó biztonságtudatossága hiányának szemléltetésére, mint minden idők legpusztítóbb vírusa/férge.

A féreg egy txt szövegállománynak álcázott Microsoft Visual Basic Script (txt.vbs) volt; ha a felhasználó kíváncsiságból rákattintott, a vírusprogram lefutott és egyrészt a felhasználó e-mail-fiókjában található összes címre szétküldte magát – pillanatok alatt megbénítva minden érintett szervezet levelezési rendszerét –, másrészt letörölte vagy felülírta az .mp3 kiterjesztésű fájlokat. Számos fájltípusnál a kiterjesztéshez hozzátett egy .vbs kiterjesztést, átírta a registry beállításokat, és végül, de nem utolsó sorban letöltött egy trójai programot. Két nap alatt több mint 45 millió számítógépet fertőzött meg, és világszinten szinte minden elektronikus levelezést használó szervezetben károkat okozott, mind a beprogramozott funkcióinak lefutásával, mind a hatalmas levéláradat okozta rendszerleállásokkal, szolgáltatáskiesésekkel. Ezen felül további költséget jelentett a szervezeteknek a károk helyreállítása, az incidens utóhatásainak csillapítása, a nyomozások és a folyamatok felülvizsgálata, a technológiai és egyéb kontrollok javítása.

Nem szükséges a „szerelemvírus" teljes történetét és részletes funkcionalitását lejegyezni, ezt számos tanulmány és cikk megtette már, viszont azokat a kulcsmomentumokat mindenképpen ki kell emelni, amelyek tipikusak, és amelyekre egy információbiztonsági oktatás vagy tudatossági kampány során kiemelten fel kell hívni a felhasználók figyelmét. Gondolok itt végrehajtható állományok e-mailben való közlekedtetésének engedélyezésére/tiltására, az e-mail-tartalomszűrő megoldások alacsony penetrációjára (megjegyzem, ez még most, 2017-ben sincs mindenhol) és legfőképp arra, hogy a felhasználók nem voltak felkészülve egy szöveges állománynak álcázott script fájl felismerésére. Annak a fajta incidenskezelési tudatosságnak a kialakítása, amelyet jelen tananyag is céloz, sajnos még a mai napig erős hiányossága a szervezetek többségének.

A másik ilyen eset, amely szintén a felhasználói figyelmetlenségen múlott, már sokkal komolyabb károkat okozott nemcsak a megtámadott és történetesen információvédelmi megoldásokat gyártó cégnek, hanem ezen megoldásokon keresztül a cég ügyfeleinek is.

Név nélkül, csak a releváns és a felhasználókat érintő kérdésekre fókuszálva, az alábbiakat lehet tudni. A támadók nagy valószínűség szerint közösségi oldalakon gyűjtöttek információkat

a megtámadandó cég alkalmazottjainak kiválasztásához. Ezután a kiszemelt áldozatoknak adathalász leveleket küldtek, amelyekben olyan Excel fájlok voltak, amelyek 0day Flash exploitot tartalmaztak. A felhasználók a csatolt fájlra rákattintva tudtukon kívül telepítettek egy távoli hozzáférést biztosító programot a gépre, amely ezen funkcióján kívül felhasználói bejelentkezési adatokat is elkezdett gyűjteni. A bejelentkezési adatokkal és a távoli hozzáférési lehetőséggel aztán a támadók további rendszerekhez fértek hozzá, többek között olyan bizalmas adatokhoz, amelyekkel más ügyfelek rendszereiben ki tudták cselezni a kétfaktoros authentikációs védelmet. A kár több tíz millió dollár volt, és jelentősen rontotta a szervezet megítélését és piaci helyzetét, illetve az eset után is szerepeltek a hírekben olyan adatlopási incidensek, amelyek eredete erre az esetre volt visszavezethető.

A fenti két példa is jól mutatja, hogy az ember kulcsfontosságú szereplő e kérdéskörben, még akkor is, ha egy kontrollintézkedésekkel jól körbebástyázott szervezetről beszélünk.

7.1.1. PPT – People, Process, Technology

Emberek, folyamatok, technológia. A fenti hármas fogalomegység rengeteg szervezet működésének alap építőköve. Nem kivétel ez alól az információvédelem sem.

7.1.1.1. People

Biztonság és információvédelem szervezete, funkcionális csoportjai

Egy szervezetben mindenki felelős az információvédelemért. Nem mindenkinek ugyanaz a feladata, de tekintve, hogy a szervezetek működésének mindig van egy vagy több célja, és az ott dolgozók ezen cél – célok megvalósulásában játszanak fontos szerepet, ez ugyanúgy vonatkozik a szervezeti információk védelmére is. Hasonlóan, ahogy mindenkinek kötelessége védeni a fizikai értékeket (épületek, autók, berendezési tárgyak, stb.) ugyanígy gondoskodni kell az információs vagyon biztonságáról is. Ennek érdekében a szervezetekben ki kell alakítani az információvédelemért felelős szervezeti egységet és hierarchiát, valamint rögzíteni kell a vonatkozó szabályzatokban és személyes dokumentumokban (például munkaszerződés, munkaköri leírás), valamint szerződésekben az érintettek feladatait és felelősségeit az információvédelem kapcsán.

A szervezet vezetője

Ahogy a 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról is előírja: „6. A szervezeteknek az elektronikus információs rendszereik védelmét biztosító kötelezettségei

11. § (1) A szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről […].”[1]

A jogszabály felsorolja, mi mindent kell megtenni a szervezeti vezetőnek az információs rendszerek védelmével kapcsolatban. Ezt nem soroljuk fel most részletesen, csak gyakorlati oldalról közelítjük meg a kérdést. A szervezet vezetője az alábbi tevékenységekkel tudja a legnagyobb segítséget nyújtani a szervezet információvédelméhez:

- Elegendő anyagi és humánerőforrást biztosít a terület részére.
- Ha egyes biztonságot érintő kulcsprojekteket a személyes támogatásával is előrelendít (vezetői levél, részvétel a projektirányító bizottságban, projektszponzori szerep vállalása).

[1] https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1300050.tv (a letöltés ideje: 2017. április 20.)

- Rendszeres beszámolási kötelezettséget ír elő az egész biztonsági és információbiztonsági terület részére.
- Kockázatmenedzsment-rendszer keretében figyelemmel kíséri a szervezet biztonsági és információbiztonsági kockázatait.
- Működteti a Következménymenedzsment-rendszert (erről lesz még szó később).
- Támogatja a biztonságtudatossági kampányokat (vezetői levél, megjelenés a rendezvényeken, a belső kommunikációban, részvétel a nyitó és záró rendezvényeken).

Fontos, hogy a szervezet lássa és érezze, hogy a felsővezetés szem előtt tartja az egész szervezet információbiztonsági állapotát.

A szakértők

A szervezetben az információbiztonsági szakértők azok, akik kialakítják és működtetik az információbiztonsági irányítási rendszert. Az ő feladatuk a szabályozói környezet megteremtése, a megfelelő folyamatok kialakítása és a kockázatmenedzsment-rendszer információbiztonsági vonalának működtetése. Továbbá ők találják ki és valósítják meg a biztonsági oktatások és tudatossági kampányok szakmai részét. Feladataik közé tartozik még az információbiztonsági technológiák megtervezése és bevezetése, valamint – amennyiben van elegendő erőforrás – a működtetésük is. A szakértők dolga a kontrollkörnyezet ellenőrzési rendszerének működtetése is.

Tekintve, hogy sok szervezetben gyakran egy fő – a jogszabály által is előírt –információs rendszer biztonságáért felelős személy áll rendelkezésre, önmagában ez az egy fő nem elegendő arra, hogy az összes szakértői feladatot ellássa és működtesse. Ilyen esetekben javasolt külső szakértők igénybe vétele, akik rendelkeznek a megfelelő szakmai képesítésekkel, tapasztalattal, és ki tudják pótolni a hiányzó erőforrást vagy adott esetben a hiányzó szakértelmet.

Üzemeltetők és fejlesztők

A szervezetek folyamatainak nagy részét ma már informatikai rendszerek támogatják, ezért ezek fejlesztőire és üzemeltetőire különösen nagy felelősség hárul. Manapság már nem elegendő, hogy egy rendszer működik, az is követelmény, hogy mindezt biztonságosan tegye. A rendszerek alapbeállításai jellemzően nem a legbiztonságosabb működést fogják biztosítani, ezért szükséges, hogy az üzemeltetők a szakértőkkel közösen kialakítsák az informatikai rendszerek megerősítését (hardening), áttekintsék és dokumentálják a biztonsági beállításokat, és rendszeresen mérjék, teszteljék a biztonsági követelményeknek való megfelelést. Ezen tevékenységet az Egységes Európai Adatvédelmi Rendelet (GDPR)[2] 32. cikkének „Az adatkezelés biztonsága” d. pontja is előírja: „ideértve, többek között, adott esetben d. az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.”

Fejlesztések esetén fontos, hogy a szakértők meghatározzák az alkalmazásfejlesztés biztonsági követelményeit, és a fejlesztés legkorábbi fázisától már ezek figyelembe legyenek véve.

Nagyon fontos, hogy a fejlesztők, üzemeltetők és a biztonsági szakértők hatékonyan tudjanak együttműködni. Ennek érdekében javasolt heti rendszerességgel olyan megbeszélést szervezni, ahol az érintettek egyeztetni tudnak a fennálló közös ügyekről, projektekről, fejlesztésekről, esetleges problémákról, audit pontokról.

---

[2] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

A felhasználók mint kulcsszereplők az egyes területeken

A felhasználóknak kulcsszerepe van az információbiztonság fenntartásában, hiszen ők azok, akik nap mint nap, ténylegesen hozzáférnek az adatokhoz, informatikai rendszerekhez. Ők azok, akik az adatokat előállítják, továbbítják, különböző informatikai eszközökön letárolják vagy adathordozókon hordozzák, majd az adatot megsemmisítik, ha ez szükséges. Fentiekből következően felhasználónak minősül mindenki, legyen vezető, üzemeltető, szakértő vagy külsős, aki hozzáfér a szervezet adataihoz. A legfontosabb, hogy a felhasználók tisztában legyenek a fenyegetettségekkel, a szabályokkal, valamint azzal, mit is kell tenniük, hogy megelőzzék az információbiztonsági (és egyéb biztonsági) incidenseket, vagy ha megelőzni nem is sikerül, időben felismerjék azokat és tudják, milyen csatornán lehet jelenteni azt az illetékesek felé.

Ezen ismereteket oktatásokkal és biztonságtudatossági kampányokkal lehet a felhasználók részére átadni. Ezek szervezésével külön fejezet foglalkozik.

A céges biztonsági és az információvédelmi kultúra kialakulása

Egy szervezetben a megfelelő szintű biztonsági és információvédelmi kultúra kialakítása nem megy egyik napról a másikra. Egyrészt a szervezet folyamatosan változik, és ezzel együtt változnak a szervezeti célok, a szervezeti felépítés, valamint változnak az informatikai rendszerek és van fluktuáció, tehát az információvédelmi rendszer szereplői, személyei is változnak.

Még ha a szervezet vezetése komolyan is veszi azt a kihívást, hogy egy elfogadott kockázati szinten működő szervezetet működtessen, és elegendő pénzt és erőforrást biztosít, akkor is gondos tervezés és kitartás szükséges a hosszú évek alatt annak az állapotnak az eléréséhez, hogy a szervezeti célok, a felhasznált erőforrások és a viselt kockázatok elfogadható szinten legyenek. Nem véletlen, hogy a 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (továbbiakban Ibtv. törvény) is két évet ír elő a szervezeteknek az egyes biztonsági szintek elérésére.

A fent leírtak oka, hogy a szervezetek napi működése, működtetése, az alapfolyamatok ellátása is jellemzően kihívásokkal teli, ezért nem lehet a teljes biztonsági kontrollrendszert egyszerre bevezetni, és minden védelmi technológiát elindítani. Természetesen a felhasználók fejében sem fog csettintésre világosság gyúlni, és nem fogják egy oktatástól minden eddigi rossz beidegződésüket elfelejteni, és a továbbiakban tudatosan cselekedni. Ez hosszú évek munkája.

A szervezeti alapműködés biztosítása és a rossz beidegződések, gyakorlatok megszüntetése sokszor konfliktusokkal jár, amit biztonsági felelősként fel kell vállalni – ehhez persze szükséges a felsővezetés támogatása. Konfrontációra lehet számítani a felhasználók részéről, az alaptevékenységet működtető szakmai és üzleti területek részéről, adott esetben az IT üzemeltetés részéről is. Szokták mondani, hogy a biztonság és a funkcionalitás egymással ellentétes vektorok, de mindenképpen törekedni kell optimális megoldásra. Erre szolgál a kockázatmenedzsment. Fontos, hogy biztonsági területként ne feltétlen tiltsunk (azonnal). Sokkal kézenfekvőbb, ha egy-egy kockázatos döntés, beruházás, funkció bevezetés stb. előtt elemezzük a kockázatokat, és egy ad hoc kockázatelemzésben a döntéshozók elé tárjuk a lehetőségeket. Majd megkérjük őket, döntsék el, mekkora kockázatot vállalnak fel az adott megoldás bevezetésével. Fontos, hogy ahhoz, hogy idáig eljussunk, léteznie kell a kockázatmenedzsmentnek mint folyamatnak.

7.1.1.2. Process

Biztonsági és információvédelmi folyamatok, a szervezet szabályozói alapján

A biztonsági és információvédelmi folyamatok rögzítve vannak számos nyilvánosan elérhető dokumentumban. Államigazgatásban a 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, valamint a 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről (továbbiakban 41/2015-ös BM rendelet) jogszabályokban vannak leírva a folyamatok és megvalósítandó eljárások. Nem államigazgatási szervezetek pedig választhatnak több kiváló keretrendszer közül.

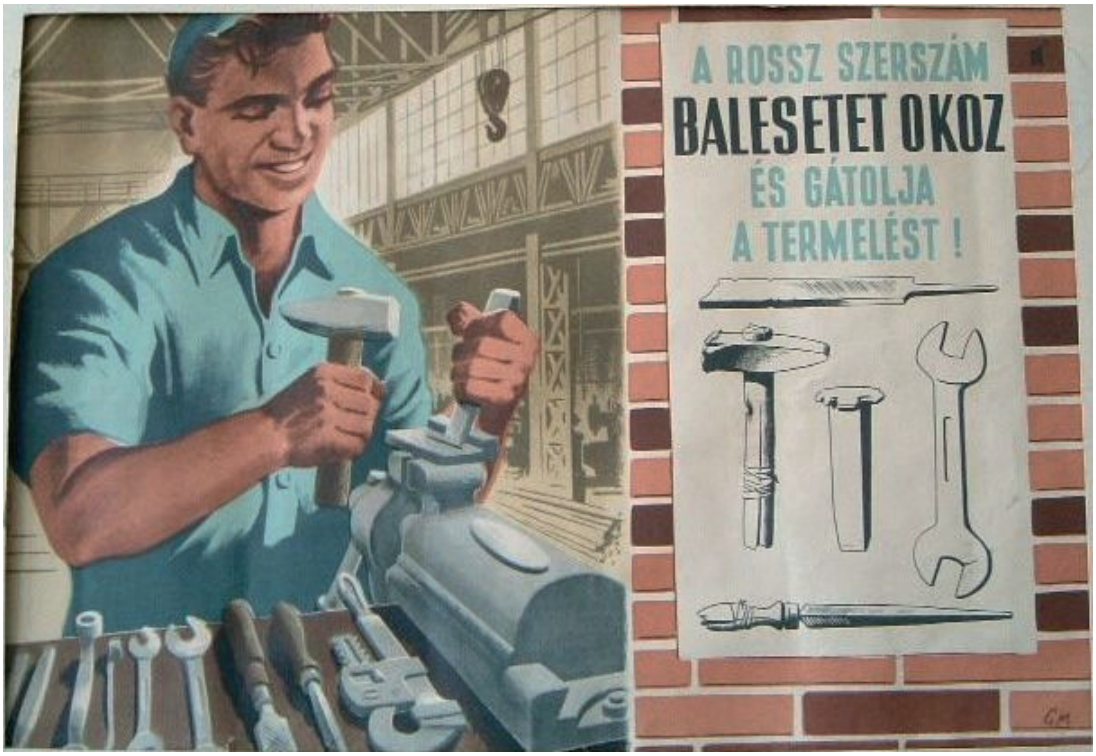
Az egyik ilyen az ISACA (Information Systems Audit and Control Association) által gondozott COBIT – Control Objectives for IT and Related Technology. A Cobit két fő területen (Governance of Enterprise IT és Management of Enterprise IT) 5 domainben 37 folyamatot rögzít, amelyeket, ha végig követ és bevezet egy szervezet, egy hatékonyan és biztonságosan működő biztonságirányítási rendszert tudhat magáénak.

A másik az ISO27000 szabványcsalád. Ez a legjobb gyakorlatokat fogalmazza meg az információvédelem számos területére vonatkozóan, a kockázatmenedzsmenttől a hálózati és alkalmazásbiztonságon keresztül a beszállítókkal történő kapcsolatra vonatkozó biztonsági követelményekig, és még sok egyéb témában. A leggyakrabban alkalmazott szabványokat az ISO27001 tartalmazza. E révén többek között azon követelmények érhetők el, amelyek alapján a szervezet tanúsítást szerezhet a szabványban foglalt követelményeknek történő megfelelés igazolására. A másik ilyen szabvány, amely alapján nem lehet ugyan tanúsítványt szerezni, de a tartalma segít a szervezetnek a megfelelő folyamatok és legjobb gyakorlatok kialakításában, az az ISO 27002, ami a javasolt biztonsági kontrollok és legjobb gyakorlatok gyűjteménye.

Természetesen a fentieken kívül számos szervezetnek vannak olyan dokumentumai, amelyek az információvédelemmel kapcsolatos kontrollokat és folyamatokat írnak le. Ilyen egyebek mellett a SANS Institute, a NIST (National Institute of Standards and Technology), a CIS (Center of Internet Security), a CSA (Cloud Security Alliance). Ezen szervezetek rengeteg olyan anyagot publikálnak, amelyek segítenek, ha valaki akár technológiákat, akár folyamatokat akar bevezetni, és ebben segítségre szorul.

Tudatosság, információvédelmi attitűd és feladatok a mindennapokban, mind a munkahelyen, mind munkahelyen kívül

Hiába várjuk el felhasználóktól, hogy megfelelően védjék egy szervezet információs vagyonát és eszközeit, ha e kérdésben nem tudatosak. A tudatosság nem alapkészség, ezt ki kell alakítani. Régen, amikor még nem voltak számítógépek, hanem szerszámokkal, egyéb gépekkel és berendezésekkel dolgoztak az emberek, akkor is megvoltak a biztonságtudatosság formálásának eszközei. Ugyanúgy, ahogy manapság, régen is voltak oktatások, képzések a gépek és berendezések megfelelő és biztonságos használatáról. Ezek célja egyrészt a munkások és dolgozók testi épségének megóvása volt, másrészt pedig a szervezet vagyonának a védelme, hiszen már régen is dolgoztak nagyértékű gépekkel, és egy-egy baleset vagy a nem szakszerű működtetésből származó meghibásodás a termelés leállását és így bevételkiesést – mai szakszóval élve üzletmenet-folytonossági incidenst – okozott. Ezek elkerülése érdekében oktatásokat és kampányokat szerveztek régen is, valamint plakátokkal és táblákkal hívták fel a dolgozók figyelmét a potenciális vészhelyzetekre.

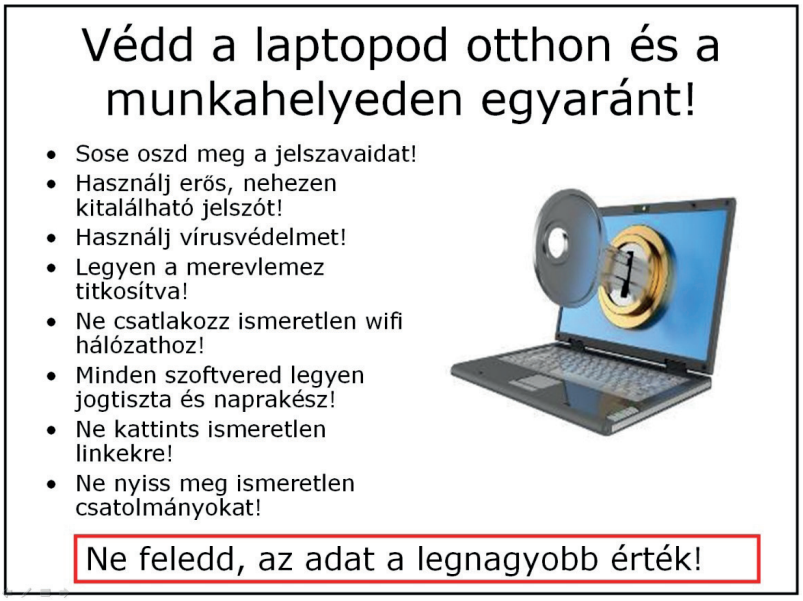


1. ábra

Munkavédelmi és üzletmenet-folytonossági plakát a hatvanas évekből

Forrás: http://www.ommf.gov.hu/nagyitas.php?img=421.jpg

Manapság, amikor majdnem minden üzleti és ügyviteli folyamatot számítógép támogat, és az interneten keresztül zajlik a kommunikáció, hasonlóképpen tudatosítani kell a veszélyeket. A plakát mint módszer ugyanolyan hatékony, mint régen, de természetesen nem ez az egyetlen eszköz a figyelemfelhívásra, jelen tananyag *Eszközök a munkavállalók figyelmének felkeltésére, fenntartására, motiváció, buy-in, lessons learned* című része is még számos módszert és lehetőséget bemutat



2. ábra

Biztonságtudatossági plakát – példa

Forrás: A szerző saját szerkesztése

A biztonságtudatossági kampányoknál fontos, hogy a felhasználót szembesítsük azzal, hogy ugyanazt a technológiát használja otthon és a munkahelyén, és jellemzően ugyanazok a fenyegetettségek is tekinthetők potenciálisnak. Ezért ha sikerül arra rámutatni, hogy az otthoni adatait és informatikai eszközeit saját jól felfogott érdeke védeni, akkor könnyen rá lehet vezetni, hogy a munkahelyén is hasonló módon járjon el. Ha ez sikerül, akkor a felhasználó sokkal könnyebben fogja megérteni és elfogadni a szervezeti biztonsági szabályokat.

Biztonsági és információvédelmi feladatok vészhelyzetben, incidens esetén

Az egyik legfontosabb kérdés az, hogy a felhasználó hogyan tudja megelőzni, felismerni, jelenteni és a legkisebb kárt okozva megszakítani az incidenst. Erről szól az *Incidenskezelés folyamata és szakaszai* című rész.

7.1.1.3. Technology

A szervezet biztonsági és információvédelmi infrastruktúrája, amiről a felhasználónak nem kell tudnia

Egy felhasználónak nem kell ismernie minden, egy adott szervezet által működtetett információvédelmi technológiát. Olyan ez, mint egy hajón a gépház: az utasoknak nem kell ismerniük a működését, sőt nem is szabad még csak a közelébe sem menniük. Ugyanez igaz a szervezetek biztonsági infrastruktúrájára. Vannak olyan eszközök, amelyek alkalmazása, típusa vagy architektúrája eleve védendő információ, valamint a felhasználók nagy többsége nem is rendelkezik olyan mély informatikai ismeretekkel, amelyek szükségesek ezen rendszerek működésének megértéséhez. Mind a felhasználónak, mind az IT üzemeltetőnek és a többi szereplőnek meg kell értenie, hogy az információvédelmi infrastruktúra alapvetően az ő érdeküket szolgálja, még akkor is, ha bizonyos tevékenységeket tilt vagy korlátoz. Az egyik legegyszerűbb példa, hogy a rendszerekben a tevékenységek naplózása védi mind a felhasználót, mind az informatikust, hiszen, ha például csoportfelhasználót használnak, és ezen csoportfelhasználó nevében történik valamilyen biztonsági esemény, akkor potenciálisan mindenki gyanússá válik, aki ismerte és használta ezt a usert. Ezért is fontos, hogy mindenki azonosított és hitelesített módon használja a rendszereket, vigyázzon a jelszavára vagy hitelesítő eszközére. Ugyanakkor a felhasználónak nem kell tudnia, hogy hogyan működik például egy tanúsítvány alapú azonosítás és hitelesítés.

Végfelhasználókat is érintő biztonsági és információvédelmi infrastruktúrák, alkalmazások és funkciók, amelyekkel mindenkinek tisztában kell lennie

Rengeteg folyamat, kontroll és technológia van jelen folyamatosan a szervezeteknél. A felhasználók számára a szükséges és elégséges tudást kell átadni. Erre célszerű egy kifejezetten a felhasználói feladatokat, felelősségeket és fenyegetettségeket tartalmazó kiadványt közzétenni, amely a hatályos biztonsági szabályozások felhasználókat érintő kivonata kell, hogy legyen. Azon oktatásokon, ahol a belső biztonsági szabályokat oktatjuk, ennek az anyagát kell részletesen elmagyarázni és számon kérni.

Ezek a teljesség igénye nélkül:

- végpontvédelem, vírusvédelem;
- fizikai biztonsági szabályok, belépés, benntartózkodás, belépőkártya használata;
- adathordozók kezelése;
- az internetezés és az elektronikus levelezés szabályai;

- az adat- és dokumentumkezelés, a tárolás, a továbbítás és a megsemmisítés szabályai;
- a hordozható eszközök és az okoseszközök használatának szabályai (különösen, ha saját eszközt is enged a szervezet használni a céges informatikai infrastruktúrában);
- a tiszta asztalra és tiszta képernyőre vonatkozó szabályok;
- Teendők biztonsági incidens gyanúja esetén, incidensjelentési csatornák, teendők incidens előtt, alatt és után.

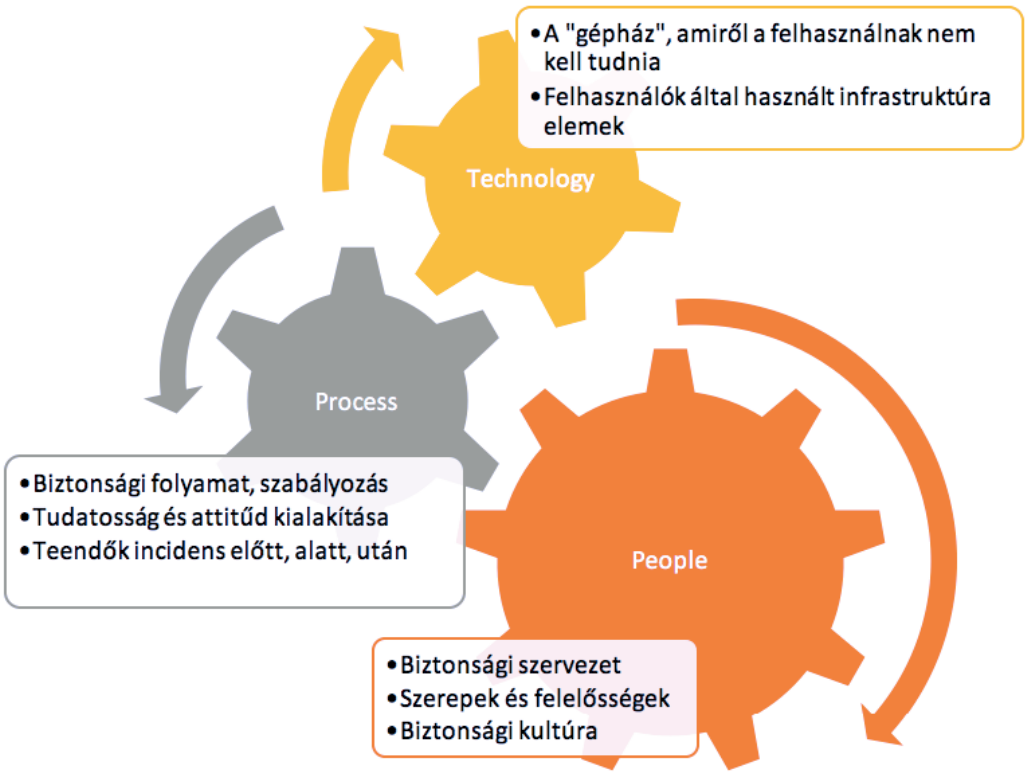
7.1.1.4. PPT, a háromlábú szék

Ha van technológia és vannak folyamatok is, de nincs meg a szükséges létszámú és képzettségű ember a szervezetben, akkor egyes szereplőkön nagy lesz a szervezeti nyomás, az információvédelem mint szempont háttérbe szorul, adott esetben a témával kapcsolatos feladatok nem vagy nem olyan precízen fognak megvalósulni, mint ahogy az elvárható lenne. Példákkal illusztrálva, ha nincs egy adott területen elegendő felhasználó, és adott esetben több ember feladatát is el kell látni, amire a normál munkaidő nem elegendő, előfordulhat, hogy a céges, akár ügyféladatokat is tartalmazó fájlokat a nem tudatos felhasználó hazaküldi magának, vagy nem titkosított adathordozóra másolja, hogy majd otthon befejezze a feladatát. Az adathordozón rajta maradnak az adatok, amely elveszhet vagy elhagyják, otthon többek által is használt informatikai környezetbe kerül, és máris sérülnek az információvédelmi alapkövetelmények. Különösen problémás, ha a felhasználó a céges információkat szándékosan juttatja ki a szervezet jól védett kontrollkörnyezetéből, mivel ilyenkor már nincsenek az adatok a szervezet felügyelete alatt, és akár illetéktelenek is hozzáférhetnek, az adat további sorsa pedig innentől kezdve követhetetlenné válik.

Ha vannak folyamatok és van ember is, de nincs megfelelő védelmi infrastruktúra, technológia, úgy könnyebben bejutnak a támadók a hálózatba, könnyebben eljutnak a kártevők a felhasználókig. Az eszközökön lévő adatokat nem lehet megvédeni, ha a hordozható eszközök nincsenek megfelelően menedzselve. Nehézkes, ha nem teljesen követhetetlen a jogosultságok kezelése, ellenőrzése – ez szorosan együtt értendő a jogosultságkezelési folyamattal.

Ha pedig van ember és van technológia, de nincsenek meg a szabályok és folyamatok, úgy senki nem tudja pontosan, mik is az elvárások. Az emberek érzésből és hangulat alapján cselekednek, az informatikai rendszerek technológiák ad hoc jelleggel, az üzemeltetők saját biztonsági attitűdjének megfelelően vannak beállítva. Ha nincsenek alapkövetelmények és folyamatok és a biztonság nem épül be a szervezet mindennapjaiba, akkor a biztonsági kontrollrendszer lyukassá válik, nem lesz egységes, ad hoc működik vagy egyáltalán nem. Ha nincsenek szabályok és követelmények, úgy sérülékeny szoftverek születnek, a rendszerek nincsenek rendszeresen ellenőrizve, nincsenek biztonságos működésre beállítva, és végül, de nem utolsó sorban nincs lehetőség számonkérésre és szankcionálásra, ha valami nem megfelelően működik.

A szervezet Információbiztonsági Felelőseinek elsődleges feladata, hogy a People–Process–Technology hármas egységet bevezessék a szervezetbe.



3. **ábra**

People (Ember), Process (Folyamat), Technology (Technológia) **hármasa**

Forrás: A szerző saját szerkesztése

Az Ibtv. és a hozzá kapcsolódó 41/2015-ös BM rendelet felépítése és szellemisége kiválóan példázza, mennyire fontos a folyamatos fejlesztés mind a három területen. Ugyan a jogszabály nem sorolja e hármas egységbe a végrehajtandó feladatokat és követelményeket, látszódik, hogy az egyes biztonsági szintekhez kapcsolódó követelmények követik a fokozatosság elvét, és nemcsak technológiát, folyamatokat, humánerőforrást és képzést írnak elő, hanem minden szinten egy megfelelően kiegyensúlyozott és megvalósítható követelménystruktúra található.

7.1.2. Biztonságtudatosság és kockázatérzékenység mint gondolkodásmód kialakítása

A biztonságtudatosság és a kockázatérzékenység alapjaiban eltérő készségek és a végfelhasználók mindkettőnek az úgynevezett kockázati mérlegelés során veszik hasznát. A *biztonságtudatosság* a fenyegetettségek ismeretét, természetét, hatásait, megelőzését és a hozzájuk kapcsolódó folyamatok ismeretét jelenti, míg a *kockázatérzékenység* egy-egy szituációban a fenyegetettség felismerésének és a rá adandó válaszlépésnek a helyes mérlegelését.

Tulajdonképpen az élet számos területén mindenki, kivétel nélkül kockázatelemzést, kockázati mérlegelést végez.

Minden esetben, amikor valamilyen kérdésben döntést kell hoznunk, mérlegelünk, felvetjük és végiggondoljuk az esetleges forgatókönyveket és lehetséges következményeket.

Kockázatelemzés lehet egy úttesten való áthaladás: mi a fenyegetettség? A közlekedő autók. Mi a lehetséges kár? Jómagam. Mi a mérlegelés? Át tudok-e úgy jutni, hogy nem ütnek el? Ha úgy döntök, átmegyek, mivel lassan és ritkán mennek az autók, akkor a fennálló kockázatot elviselhető kategóriába soroltam, mivel kicsi a bekövetkezési valószínűség, bár a potenciális kárérték nagy.

Változtassuk meg a vizsgálandó paramétereket.

A bekövetkezési valószínűség növekedése: az autók nem lassan és ritkán jönnek, hanem sűrűn és gyorsan. Megnő a bekövetkezési valószínűsége annak, hogy elütnek. Ezt inkább már nem vállalom fel, és kockázatcsökkentő intézkedésként keresek egy hivatalos gyalogátkelő helyet, ahol lámpával van védve az áthaladásom.

A potenciális kárérték növekedése: a gyerekem is velem van, ezért bár az autók továbbra is lassan és ritkábban jönnek, mivel nem csak magamat, hanem a gyerek életét is veszélyeztetném, ezért inkább ezt már nem vállalom fel, és kockázatcsökkentő intézkedésként keresek egy hivatalos gyalogátkelő helyet, ahol lámpával van védve az áthaladásom.

Amikor bekövetkezik egy baleset, akkor sajnos a gyalogos nem jól mérte fel a kockázatokat.

Fenti analógia ugyanúgy működik mindenre, akár a lejárt szavatosságú tej fogyasztására vonatkozóan is, vagy egy ismeretlen eredetű használt autó megvásárlására, de gondolhatunk egy ismeretlen hátterű internetes vásárlásra, egy vakrandira vagy egy új okostelefonos alkalmazás letöltésére is. A kockázatok mindig mindenhol jelen vannak, ahol olyan esemény következhet be, amely valamilyen negatív hatással lehet az egyénre vagy a hozzá kapcsolódó szervezetre vagy anyagi javakra.

Mi tehát a feladatunk és célunk a biztonságtudatossággal és a kockázattudatos gondolkodás végfelhasználókkal történő megismertetésével? Az, hogy a szervezetünkben működő felhasználók ismerjék a munkájuk során őket fenyegető veszélyeket, és amikor szembekerülnek velük, felelős mérlegeléssel tudjanak dönteni arról, mit is kezdjenek az adott helyzettel. Ha már azt elérjük, hogy a végfelhasználó – ha ő maga nem is tudja mivel áll szemben –, a teendőkről inkább megkérdezi a szakértőket (mondjuk a szervezet információvédelmi felelősét), már egy hatalmas lépést tettünk a szervezeti információk és informatikai rendszerek megóvása érdekében.

Szervezeti szinten az egyén biztonságtudatossága nem fejleszthető, csak szervezett formában. Ahhoz, hogy egy szervezet eljusson oda, hogy biztonságtudatossági oktatásokat és kampányokat szervezzen, elengedhetetlen, hogy a szervezet egésze, beleértve a vezetést is, támogassa ezen kezdeményezéseket. Vagyis elengedhetetlen, hogy a biztonság és az információvédelem a szervezeti kultúra részévé váljon.

7.1.3. A kockázatérzékenységnek és a biztonságtudatosságnak mint a szervezeti kultúra részeinek kialakítása a szervezetben

Minden felhasználó más és más információbiztonsági szocializációval érkezik a szervezethez. Mást látott és hallott otthon, mást az iskolai tanulmányai során, és az egyes cégeknél is nagyon különböző információvédelmi céges kultúra jellemző. Elmondható, hogy a multinacionális vállalatoktól érkező kollégák általában érettebbek e tekintetben. Ilyen környezetben – akár meglévő jogszabályi háttér miatt, akár még a multinacionális céggé válás időhorizontján – a cégvezetés hamarabb felismerte az információvédelem jelentőségét, és ennek megfelelő kontrollkörnyezetet alakítottak ki, a felhasználók képzését is biztosítva. Mindez egy kisvállalatra, de nagyon sok középvállalatra sem jellemző mind a mai napig.

A szervezet legfelső vezetésének dolga a biztonságtudatosság kialakítása, és övék általában a szervezet biztonságáért való felelősség is.[3] Ahhoz, hogy a szervezet vezetőségén túl az egyes funkcionális területek is a megfelelő hatékonysággal tudják végezni a feladataikat, elengedhetetlen a szervezet vezetésének akaratnyilvánítása a biztonság és az információvédelem megteremtése és szinten tartása, a kockázatok kezelése iránt, valamint, hogy fentiekhez deklaráltan biztosítva legyenek a megfelelő erőforrások.

---

[3] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. 6. A szervezeteknek az elektronikus információs rendszereik védelmét biztosító kötelezettségei -
11. § (1) A szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről a következők szerint: (2) Az (1) bekezdésben meghatározott feladatokért a szervezet vezetője az (1) bekezdés k) és l) pontjában meghatározott esetben is felelős, kivéve azokat az esetköröket, amikor jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltatót, illetve központi adatkezelőt és adatfeldolgozó szolgáltatót kell a szervezetnek igénybe venni.

7.1.3.1. Biztonsági politika, információbiztonsági politika, vezetői felelősségvállalás

Ezen deklarációt egy úgynevezett *biztonsági politikában,* ha szűkebben értelmezzük, úgy *információbiztonsági politikában* szokás megfogalmazni, amely hasonlatos az ISO9001-es minőségirányítási rendszerek minőségpolitikájához. Bár maga a dokumentum mint *politika* (Security Policy, Information Security Policy) számos szabványban megjelenik, nincs egységes és részletes minimumkövetelmény a tartalommal kapcsolatban. A tartalom részletezettsége szervezetenként változik: van, ahol a biztonsági politika rövid, egy – maximum három oldalas, van ahol ez egy sokkal részletesebb, sok területre követelményeket meghatározó dokumentum, amely tartalmazhat kockázatkezeléssel vagy a biztonsági szervezet felépítésével kapcsolatos elemeket is.

Ugyanakkor figyelembe kell venni, hogy végső soron a cél, a felsővezetői támogatás deklarálása. Enélkül sokszor sajnos maguk a szervezeti vezetők és a felhasználók sem veszik komolyan a biztonságot és az információk védelmére irányuló erőfeszítéseket.

Egy biztonsági politika fő tartalmi elemei (a kötelező formai elemeken – célja, tárgya, hatálya, a felülvizsgálat, a jóváhagyók stb. – kívül) a következők:

- a biztonság mint állapot megteremtésére és fenntartására, a kockázatok elfogadható szinten tartására vonatkozó vezetőségi akaratnyilvánítás;
- a biztonsági és információbiztonsági alapelvek;
- a biztonsági és információbiztonsági célkitűzések;
- a biztonság és információbiztonság szervezete;
- a kockázatmenedzsment.

7.1.3.2. Kockázatmenedzsment mint a szervezeti biztonságtudatosság mozgatórugója

Ha egy szervezetben nem működnek kockázatmenedzsment-folyamatok, az egész kontrollrendszer ad hoc működik, az egyes szervezetek és vezetőik aktuális kockázatérzékenysége (vagy –érzéketlensége) szerint. Ez rendkívül veszélyes, mert ilyenkor jellemzően a szervezet nem a valós kockázatokra reagál. Adott esetben túlköltekezik, vagy éppenséggel nem a megfelelő erőforrás-mennyiséget biztosítja a kontrollokhoz. Ezen kívül, ha működnek is kontrollok, azok hamis biztonságérzetet adnak a szervezetnek, s ebbe már sokan belebuktak.

Nem kitérve részletesen a kockázatmenedzsment-folyamatokra, annyit fontos tudni, hogy a kockázatok mérése, értékelése és monitoringja, valamint ennek vezetői fókusza adja azt a körforgást, ami miatt a szervezet minden területe előbb-utóbb bekapcsolódik a kontrollrendszer működtetésébe. Ahol a kontrollokat nem vagy nem megfelelően működtetik, a kockázati szint meg fog emelkedni, ami pedig a monitoringrendszeren keresztül – például egy negyedéves kockázati riportként – el fog jutni a felsővezetői döntéshozói testület elé. Ez a szerv – mivel végső soron a vezetőség felel a biztonságért – meg fogja tenni azokat a lépéseket, amelyek szükségesek a kockázatok kezeléséhez, ez pedig a szervezeti vezetőkön keresztül visszahat a végfelhasználókra is.

7.1.3.3. Következménymenedzsment mint a kockázatmenedzsment mozgatórugója

Következménymenedzsment nélkül nincs hatékony kockázatkezelés. Tudomásul kell venni, hogy az információvédelemmel és úgy általában a biztonsággal jellemzően akkor foglalkoznak, ha vagy nagyon tudatos és kockázatérzékeny a szervezeti vezető, vagy ha egyéb okok kényszerítenek.

Ilyen „egyéb ok” a következménymenedzsment. Ha egy szervezeti egységnél a belső vagy anyavállalati ellenőrzés, a felügyelet, a hatóság vagy valamilyen biztonsági terület problémát észlel, nem megfelelőséget, valamely kontroll- vagy biztonsági folyamat nem megfelelő működését, akkor ennek mint audit pont vagy kockázat be kell kerülnie egy olyan nyilvántartásba, amely tételesen felsorolja

ezen megállapításokat, a hozzájuk kapcsolódó kockázatkezelési feladatokat, felelősségeket és határidőket.

Ettől a két dologtól – a határidőktől és a felelősségtől – sajnos rengetegen irtóznak egyes szervezeteknél. Azonban, ha a feladatok felelősségekkel és határidőkkel vannak nyilvántartva, és a felső vezetés ezt rendszeresen áttekinti, úgy az alapok megvannak. Fontos, hogy a határidő és a felelősség ne csak rögzített információk legyenek. A szervezetnek meg kell határoznia és következetesen be is kell tarttatnia azon szankciókat, amelyek egyrészt a biztonsági és egyéb belső szabályok megsértéséért, másrészt, amelyek a kockázatkezelési intézkedések és audit pontok végrehajtásához kapcsolódó késésekért, a határidőcsúszásokért, a nem megfelelő teljesítésért járnak.

Ez olyan mozgatórugója a szervezet minden vezetői és beosztotti szintjének (akár az alvállalkozóknak is), amelynek köszönhetően mindenki komolyan fogja venni a feladatokat. Kiegészítve a következménymenedzsmentet egy jó oktatási és tudatosítási rendszerrel, elérhetők lesznek a biztonsági politikában megfogalmazott célok.

7.1.4. Az oktatás és a tudatosítás megjelenése a vonatkozó hazai jogszabályokban és a nemzetközi szabványokban

Manapság az Ibtv.-vel kapcsolatban hangzik el leggyakrabban, hogy az végre az információvédelemmel kapcsolatos olyan anyag, amelyhez az államigazgatási és önkormányzati területen dolgozó információvédelmi szakemberek igazodhatnak. Ugyanakkor nem szabad megfeledkezni az Informatikai Tárcaközi Bizottság ajánlásairól, illetve a Közigazgatási Informatikai Bizottság 25. számot viselő ajánlássorozatáról, amelyek az 1990-es évektől az Ibtv. megszületéséig számos olyan információvédelemmel és IT biztonsággal kapcsolatos előírást meghatároztak, amelyeket nemcsak a kormányzat és az államigazgatás, de a versenyszféra is igazodási pontként tartott számon.

7.1.4.1. ITB ajánlások

Alapvetően két olyan ajánlás volt, amit a kilencvenes évek kezdetétől leggyakrabban használtak az akkor még kisebb létszámban létező szakértők: a 8. és 12. számúak. Ezek rövid összefoglalója olvasható a következő sorokban:

„A Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) Informatikai biztonsági módszertani kézikönyv címet viselő, 1994-ben kiadott MeH ITB 8. számú ajánlása a brit kormány Központi Számítógép és Távközlési Ügynökség (Central Computer and Telecommunications Agency) CCTA Risk Analysis and Management Method és az északRajna vesztfáliai kormány Informationtechnik Sicherheitshandbuch felhasználásával, valamint az EU informatikai ajánlásai és a hazai jogszabályok alapján készült. A kézikönyv tájékoztatja az intézmény szervezetének vezetőségét az informatikai biztonság megteremtésének legfontosabb elemeiről, és célja felkészíteni a szervezetet az informatikai biztonsági koncepciójának kialakítására. A biztonsággal kapcsolatos legfontosabb tudnivalók, valamint az informatikai biztonság és a szervezet összbiztonsága közötti összefüggések meghatározó elemei a kézikönyvhöz csatolt mellékletekben találhatók meg."

Ugyan a 8. számú ajánlás egy CRAMM alapú kockázatelemzési módszertan, itt is megjelenik az oktatás szükségessége, mégpedig az 1.4. számú, *Vezetői feladatok az informatikai biztonsági projektben* című részben: „A munkatársak beiskolázása, oktatása és információkkal való ellátása szükséges előfeltétele a biztonsági intézkedések elfogadásának."[4]

„A Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága 1996-ban adta ki 12. számú ajánlását az „Informatikai Rendszerek Biztonsági Követelményei" címen. Ez a dokumentum lefedi

[4] A Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottságának ajánlásai 7. 1. Informatikai biztonsági módszertani kézikönyv (8. sz. ajánlás)

az informatikai biztonság egészét, azaz az adminisztratív, a fizikai és a logikai védelem területeit. Az ajánlás komplex szemléletéből adódóan kiterjed mind az informatikai rendszer környezetére, mind magára az informatikai rendszerre. A 12. sz. ajánlás az érvényes hazai jogszabályok, szabványok, valamint a hazai és nemzetközi ajánlások elsősorban az ITSEC figyelembevételével reális és megbízható alapot nyújt egyrészt a működő, másrészt a megvalósítás előtt álló informatikai rendszerek és környezetük fizikai, logikai és adminisztratív védelmi követelményeinek konkrét megfogalmazásához, a védelmi rendszerek továbbfejlesztéséhez, illetve megvalósításához."[5]

A 12. számú ajánlásban a *Személyek* című fejezetekben van előírva, hogy a munkatársakat oktatni kell. Az oktatás és a biztonságtudatosság mint védelmi intézkedés láthatóan kezdettől fogva minden biztonsági vezető eszköztárába bele kellett, hogy tartozzon.

7.1.4.2. Közigazgatási informatikai bizottság 25. számot viselő ajánlássorozata

Több mint tíz évvel az Informatikai Tárcaközi Bizottság ajánlásai után 2008-ban felülvizsgálták és aktualizálták azokat a megváltozott konrtollhoz és a fenyegetettségi körülményekhez igazodva. Kiadták a Közigazgatási Informatikai Bizottság 25. számot viselő ajánlássorozatát, Magyar Informatikai Biztonsági Ajánlások (MIBA) név alatt. Az ajánlássorozat az alábbi elemekből áll.

- 25/1 – Magyar Informatikai Biztonság Irányítási Keretrendszer (MIBIK);
- 25/1-1 – Informatikai Biztonság Irányítási Rendszer (IBIR);
- 25/1-2 – Informatikai Biztonság Irányítási Követelmények (IBIK);
- 25/1-3 – Az Informatikai Biztonság Irányításának Vizsgálata (IBIV);
- 25/2 – Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS);
- 25/3 – Informatikai Biztonsági Iránymutató Kis Szervezeteknek (IBIX).

Tekintve, hogy az ajánlássorozat is nemzetközi módszertanokat követ, és a korábbi Informatikai Tárcaközi Bizottság ajánlásaira épül, az *oktatás* és *tudatosság* számos helyen megjelenik a dokumentumokban.

7.1.4.3. A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

Az Ibtv. is fontos elemként – védelmi intézkedésként – tekint az oktatásra és a biztonságtudatosság fejlesztésére. Azzal, hogy a korábban kormányzati ajánlásként megjelent dokumentumok szintjéről törvényi szintre emelkedett az információvédelemmel kapcsolatos követelményrendszer, az oktatás és tudatosítás is ugyanolyan törvényi előírásként kérhető számon, mint bármilyen más jogszabály. Míg korábban jellemzően ez a terület sérült, ha a szervezeteknél forráshiány merült fel, most már ugyanolyan körültekintéssel kell végezni ezt a tevékenységet is, mint a többi törvény által előírtat. Idézet a törvényből:

„6. A szervezeteknek az elektronikus információs rendszereik védelmét biztosító kötelezettségei

11. § (1) A szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről a következők szerint:

[…]

g) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról, […]."[6]

---

[5] Muha Lajos (2003): *Szabványok és ajánlások az informatikai biztonság területén*. Előadás-összefoglaló. 7. A Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottságának ajánlásai 7. 1. Informatikai biztonsági módszertani kézikönyv (8. sz.) és 7. 2. Informatikai Rendszerek Biztonsági Követelményei (12. sz. ajánlás)

[6] a 2013. évi L. törvény az állami és önkormányazti szervek elektronikus információbiztonságáról Elérhető: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1300050.tv (a letöltés ideje: 2017. április 20.)

7.1.4.4. A 41/2015. (VII. 15.) BM rendelet

A rendelet *3.1.7. Tudatosság és képzés* című részének könnyebb átláthatósága és megértése érdekében az egyes követelményeket táblázatba rendeztük, és magyarázattal láttuk el.

1. táblázat

A 41/2015. (VII. 15.) BM rendelet Tudatosság és képzés című részének értelmezése

A jogszabály fejezetcíme	Követelmény	Magyarázat
3.1.7. Tudatosság és képzés		
3.1.7.1.	Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével és az e célt szolgáló ágazati szervezetekkel.	–
3.1.7.1.1. Az érintett szervezet:		
3.1.7.1.1.1.	az elektronikus információs rendszerhez hozzáféréssel rendelkező személyek folyamatos oktatásának, képzésének elősegítése;	Biztosítani kell az elegendő időt mind a felkészülésre, mind a szükséges képzésekre. E célból szervezni lehet tantermi frontális oktatásokat, elektronikus képzéseket és olyan kampányokat, amelyek nem a klasszikus oktatási, hanem inkább reklám és marketing módszerekkel hívják fel a figyelmet az információvédelem fontos kérdéseire.
3.1.7.1.1.2.	az ajánlott elektronikus információbiztonsági eljárások, technikák és technológiák naprakészen tartása;	Fontos, hogy mind a felhasználók, mind az üzemeltetők képesek legyen a technológiai változások követésére, az újdonságok megismerésére, külön kiemelve az új technológiák funkcionalitását és a magukkal hozott esetleges új veszélyforrásokat és kockázatokat.
3.1.7.1.1.3.	a fenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó legfrissebb információk megosztása érdekében kapcsolatot alakít ki és tart fenn az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és e célt szolgáló ágazati szervezetekkel.	Minden szervezet, amely információtechnológiát használ, előbb-utóbb szembesül azzal, hogy az alkalmazott hardver- és szoftverelemek elavulnak. Ennél rosszabb, hogy nemcsak az avulással kell törődni, hanem naprakésznek kell lenni az alkalmazott technológia sérülékenységeivel, gyengeségeivel kapcsolatban is. Folyamatosan nyomon kell követni a megjelenő sérülékenységeket, és ha azok érintik a szervezet információtechnológiai elemeit, gondoskodni kell a frissítésről. Amennyiben ez nem lehetséges (például egymástól függő verziók okán stb.), úgy egyéb védelmi intézkedésekkel kell megpróbálni csökkenteni a kockázatot. A jogszabály meghatározza azon szervezetet, amely eseti vagy rendszeres időnként figyelmeztetést ad ki sérülékenységekkel kapcsolatban. Az információbiztonsági piacon elérhetők olyan szolgáltatások, amelyekért ha fizet a szervezet, akkor testreszabottan, csak a saját infrastruktúrájával kapcsolatos információkat kapja meg, és nem kell a rengeteg, nem releváns adatot feldolgozni.
3.1.7.2. Képzési eljárásrend		
3.1.7.2.1. Az érintett szervezet:		
3.1.7.2.1.1.	megfogalmazza és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a képzési eljárásrendet, mely a képzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;	A képzéseket ütemezni kell, több okból is. Egyrészt sokszor nem lehet fizikai korlátok – például egy terem befogadóképessége – miatt az egész szervezetet egyszerre oktatni, képezni. Másrészt lehetnek olyan munkakörök, ahonnan nem lehet egyszerre az összes kollégát elengedni oktatásra. Tipikusan ilyenek az informatikai vagy az ügyeleti rendben dolgozók. A képzés tervezésével átlátható lesz az oktatási és képzési tevékenység, nyomon lehet követni, hogy mely képzések azok, amelyeknél frissítés szükséges.

A jogszabály fejezetcíme	Követelmény	Magyarázat
3.1.7.2.1.2.	a képzési eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a képzési eljárásrendet.	A képzési eljárásrendet is rendszeresen frissíteni kell, hiszen ahogy átalakul a szervezet és frissülnek a technológiák, úgy kell a képzéseknek is nyomon követniük a változásokat.
3.1.7.3. Biztonságtudatosság képzés		
3.1.7.3.1.	Az érintett szervezet annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára:	Fontos, hogy nem csak a szabályokat kell oktatni. Sőt elsősorban nem azokat kell. A felhasználóknak be kell mutatni az őket érintő releváns potenciális informatikai fenyegetéseket, majd, ha ezáltal megértették a biztonsági intézkedések fontosságát általában, akkor érdemes a szervezeti biztonsági szabályokat oktatni.
3.1.7.3.1.1.	az új felhasználók kezdeti képzésének részeként;	Mivel mindenki más környezetből érkezik a szervezethez, és a belépést megelőzően is eltérő biztonsági környezetben szocializálódott, ezért rendkívül fontos a belépőképzés. Ott, ahol a felhasználó- és jogosultságkezelő rendszer és a képzéseket támogató rendszerek megfelelően együttműködnek, ott bizonyos rendszerjogosultságokat csak akkor kaphat meg a felhasználó, ha a vonatkozó képzéseket is elvégezte. Ugyanez igaz az alap belépőképzésre, amely elvégzése szükséges ahhoz, hogy az alap rendszerhozzáféréseket megkapja a felhasználó. Egyes szervezeteknél ez a belépőképzés akár két–három hónapig is eltarthat. A szervezeteknek érdemes időt és erőforrást szánni az új belépők képzésére, hiszen ezáltal jelentősen csökkenthető a képzések hiányából fakadó hibák és biztonsági események bekövetkezésének esélye. Fontos, hogy új felhasználók nemcsak a belsős munkavállalók lehetnek, hanem minden olyan felhasználó, aki hozzáfér a szervezet informatikai rendszereihez és adataihoz. Értjük ez alatt a beszállítókat, a szerződéses munkák keretében érkező felhasználókat és akár egy ellenőrző hatóság embereit is. Külsős szervezetek által végzett auditok esetén hasznos, és pozitív képet ad a szervezet információbiztonsági kultúrájáról, ha az auditorok is részesülnek egy alap, testreszabott biztonsági képzésben. (Feltéve, ha informatikai rendszerhozzáférésekre is igényt tartanak.) Amennyiben hosszabb ideig tartózkodnak fizikailag is a helyszínen, praktikus az egyéb tűz- és – ha van rá speciális ok – a munkavédelmi alapszabályokat elmondani, a menekülő útvonalakat megmutatni.
3.1.7.3.1.2.	amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;	A szervezet, a rendszerek, a jogszabályok és természetesen a külső-belső fenyegetések is folyamatosan változnak, ezért szükséges, hogy a belépőképzés mellett minimum éves frissítő képzés keretén belül ismertessük a változásokat. Képzeljük el, hogy ha valaki mondjuk nyolc vagy tíz éve kapott utoljára biztonsági oktatást – vagy ad abszurdum nem is kapott –,hogyan tud reagálni a modern kihívásokra.
3.1.7.3.1.3.	az érintett szervezet által meghatározott gyakorisággal.	Az általánosságban éves szinten javasolt frissítő oktatások gyakorisága is növelhető, amennyiben erre szükség van. Például projekt jellegű munkáknál, ahol gyakran cserélődnek a partnerek (például alkalmazásfejlesztő cégek, projektvezetők), a projekt első fázisára előírhatunk egy rövid, a témára vagy a projektre koncentráló képzést.
3.1.7.4. Belső fenyegetés		
	A biztonságtudatossági képzés az érintett személyeket készítse fel a belső fenyegetések felismerésére, és tudatosítsa jelentési kötelezettségüket.	Itt a hangsúly az érintetteken van. Az alapképzéseken túl a szervezet egyes szerepköreiben dolgozók más-más típusú fenyegetésekkel találkozhatnak, ezért őket speciális képzésekben kell részesíteni.

A jogszabály fejezetcíme	Követelmény	Magyarázat
3.1.7.5. Szerepkör vagy feladat alapú biztonsági képzés		
3.1.7.5.1.	Az érintett szervezet szerepkör vagy feladat alapú biztonsági képzést nyújt az egyes szerepkörök szerinti felelős személyeknek:	Az általános felhasználói információbiztonsági képzésen túl speciális képzést igénylő területek: *1. Felsővezetők:* rendkívül elfoglaltak, időbeosztásuk miatt jellemzően nem tudnak az általános információbiztonsági képzéseken részt venni, ezért számukra egyedi, rövid, lényeges képzést kell biztosítani. *2. Vezetői asszisztensek:* a vezetők asszisztensei az informatikai támadások legpotenciálisabb célpontjai. Jellemzően rendelkeznek hozzáféréssel a vezetőjük felhasználói fiókjához, a levelezéshez és egyéb rendszerekhez. Gyakran előforduló, rossz gyakorlat, hogy a vezetők nem egy szakértő helyettesre, hanem az asszisztensre delegálnak döntéshozatalt igénylő feladatokat (ilyen például a beosztottak jogosultságainak jóváhagyása, felülvizsgálata). Ráadásul rengeteg bizalmas információval rendelkeznek, már csak a munkakörük miatt is. Fokozottan védendők, és fontos, hogy az információbiztonsági terület jó kapcsolatot ápoljon az asszisztensekkel. *3. Informatikusok/IT üzemeltetők:* manapság, amikor a szervezetek jelentős számú folyamatát informatikai rendszerek támogatják, elengedhetetlen, hogy az informatikai rendszerek – beleérve a biztonsági infrastruktúraelemek (tűzfalak, szerver- és végpontvédelem, behatolás detektálás, DLP stb.) – üzemeltetését végző munkatársak rendelkezzenek a legfrissebb ismeretekkel, ha kell, vizsgákkal is megerősítve. *4. Információbiztonsági szakértők és információbiztonsági felelős:* a fenyegetések és kockázatok változásai és a szervezet megfelelő, kockázattudatos működése érdekében szükséges, hogy a kontrollrendszert működtető és felügyelő szakértők is a legkorszerűbb tudással rendelkezzenek, hiszen így lehet a kockázatokat minimalizálni, illetve biztosítani a hatékony incidenskezelést és kivizsgálást. Az informatikai, de főleg a biztonsági területek képzései és a szakértői vizsgák megszerzése nagyságrendekkel többe kerülnek, mint egy átlagos felhasználói informatikai képzés. Ezt minden esetben az éves képzési tervekben jelezni kell. *5. Alkalmazásfejlesztők:* az alkalmazásfejlesztés azért speciális terület, mert a programozás során hajlamosak mind a megrendelő terület munkatársai, de a tervezők, a fejlesztők is úgy gondolni a biztonságra, mint egy modulra, amelyet önálló egységként az alkalmazásba helyezve, az biztonságos lesz. Sajnos ez nem így van. A biztonságos szoftverfejlesztés olyan folyamat, gondolkodásmód és követelményrendszer, amelynek a fejlesztés első lépésétől a projekt részének kell lennie. Minél később kerül a figyelem középpontjába, annál költségesebbé teszi az alkalmazás végső élesbe állását. Sőt, elképzelhető olyan eset is, hogy a biztonsági megfontolások kihagyásával tervezett szoftver minden biztonsági teszten elbukik, és a tervezéstől újra kell kezdeni a munkát. A biztonságos szoftverfejlesztési folyamatot (SSDLC – Secure Software Development LifeCycle) érdemes megvalósítani a szervezetben, mivel így a biztonság mint a szoftverminőség alapeleme fog megvalósulni. Nemcsak működni fog a szoftver, hanem biztonságos is lesz. Mindez életbevágó egyre több szervezet életében. *6. Üzlet- és/vagy ügymenet-folytonossági és katasztrófaelhárítási folyamatokban résztvevők:* A kríziskezelés és azon események kezelése, amelyek a szervezet működésének folyamatosságát biztosítják, speciális képzést igényelnek.
3.1.7.5.1.1.	az elektronikus információs rendszerhez való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően;	Ahogy korábban is volt róla szó, egyes informatikai rendszerekhez sokszor csak abban az esetben lenne szabad hozzáférést biztosítani, ha a felhasználó az adott képzést sikeresen elvégezte, esetleg le is vizsgázott. Manuális folyamatok esetén ez elég nehézkes, és sok a hibázási lehetőség is.

A jogszabály fejezetcíme	Követelmény	Magyarázat
3.1.7.5.1.2.	amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;	Új informatikai rendszerek bevezetése vagy funkcióváltozásokat jelentő verziófrissítések esetén nemcsak a felhasználókat, de az üzemeltetőket is megfelelő képzésben kell részesíteni.
3.1.7.5.1.3.	az érintett szervezet által meghatározott rendszerességgel.	Lásd a *3.1.7.3.1.3. az érintett szervezet által meghatározott gyakorisággal* részhez írt magyarázatot.
3.1.7.6. A biztonsági képzésre vonatkozó dokumentációk		
3.1.7.6.1. Az érintett szervezet:		
3.1.7.6.1.1.	dokumentálja a biztonságtudatosságra vonatkozó alap-, és szerepkör alapú biztonsági képzéseket;	Akár az általános biztonsági követelményeket meghatározó információbiztonsági szabályzatban, akár a felhasználó- és jogosultságkezelésről szóló szabályzatban, de rögzíteni kell, hogy mik az alapjogosultságok, amelyek bármilyen képzés nélkül hozzáférhetők, illetve mik azok az alap- és egyedi jogosultságok és szerepkörök, amelyekhez speciális oktatás, képzés, esetleg vizsga szükséges.
3.1.7.6.1.2.	a képzésen résztvevőkkel a képzés megtörténtét elismerteti, és ezt a dokumentumot megőrzi.	Akár elektronikus képzési rendszer (LMS – Learning Management System), akár papír alapú jelenléti ívről beszélünk, szükséges az auditálhatóság szempontjából, hogy igazolni tudjuk, hogy az adott képzés megtörtént, azon a hallgatók részt vettek, adott esetben le is vizsgáztak. A papír alapú dokumentumok esetében figyelemmel kell lenni arra, hogy az jellemzően tartalmazza a felhasználók aláírását is, ezért fokozottan védendő információnak minősül, amelyet elektronikus kezelésnél (szkennelés) is fokozottan kell védeni.

Forrás: A 41/2015. (VII. 15.) BM rendelet alapján a szerző saját szerkesztése

4. ábra

A szerepkör alapú, speciális képzés célcsoportjai

Forrás: A szerző saját szerkesztése

7.1.4.5. MSZ/T ISO/IEC 27001:2014

Az MSZ/T ISO/IEC 27001:2014 számú *Informatika. Biztonságtechnika. Információbiztonsági irányítási rendszerek. Követelmények* című szabvány „A" mellékletének *(Hivatkozásul szolgáló intézkedési célkitűzések és intézkedések) A7. Emberi erőforrás biztonsága* című fejezetében található *A 7.2. az alkalmazás során* című alfejezet *A 7.2.2. Információbiztonsági tudatosítás, képzés és tréning* pontja rendelkezik az oktatás, a képzés és a tudatosítás kérdéséről. Intézkedésként előírja, hogy:

„A szervezet minden alkalmazottjának és, ahol alkalmazható, a szerződéses munkatársaknak megfelelő tudatosító képzésben és tréningben, illetve a munkakörükhöz tartozó szervezeti szabályzatok és eljárások rendszeres frissítéseiben kell részesülniük."

Bár a korábban említett jogszabályok és a szabvány sem ír külön a vizsgáztatásról és a számonkérésről, az alábbiakban röviden összefoglaljuk, milyen lehetőségek vannak a képzéseken átadott tudás visszamérésére. Ez az utolsóként említett mozzanat azért fontos, hogy meggyőződhessünk arról, hogy az átadni kívánt tudásanyagot valóban megértették-e.

Fontos, hogy amennyiben az átadott tudásanyagot vissza szeretnénk mérni, ennek módjáról, esetleg időigényéről és a sikertelen visszamérés következményeiről előzetesen tájékoztatni kell a hallgatókat.

Az egyes oktatási anyagok zárásaként ellenőrző kérdéseket tehetünk fel szóban és/vagy írásban. Amennyiben a hallgatók megfelelő válaszokat adnak, elkönyvelhetjük, hogy a tudásanyag rögzült.

Amennyiben a válaszok nem megfelelők, el kell döntenünk, hogy megismételjük-e az adott tudásanyagrészt, vagy addig ismételgetjük a kérdést és a jó választ, amíg az megfelelően rögzül.

A vizsgáztatás az a módszer, amely esetén konkrét célértéket határozunk meg arra vonatkozóan, hogy mi az a szint, ami alatt nem tudjuk a hallgató tudásszintjét elfogadni. A hallgatóság – főleg felnőttképzések esetén – hajlamos elbagatelizálni a vizsgát, esetleg a résztvevők megpróbálják közösen megoldani. Természetesen minden vizsgáztatásnál nem állhat felügyelő minden vizsgázó mellett. Ugyanakkor meg bizonyos eszközökkel meg lehet próbálni a vizsgákat egyedivé tenni, így csökkentve az egymásról lesésnek, az összebeszélésnek vagy a komplett vizsgakérdéssor rögzítésének lehetőségét, és megakadályozva továbbadását későbbi vizsgázók számára.

Vizsgakérdéstár létrehozása: elektronikus vizsgáztatási rendszereknél jellemző, hogy például egy tíz kérdésből álló vizsga feladatait egy száz vagy még több elemű tárból válogatja össze a rendszer, így ugyanaz a kérdéssor jó eséllyel ritkán áll elő. Ennek köszönhetően a felhasználók nem tudják a kérdéssor helyes válaszainak rögzítésével megkönnyíteni a saját dolgukat. Ez okoz némi többletmunkát oktatói oldalról, de megéri a fáradtságot, mivel biztosítható vele, hogy a hallgató átfogó tudással rendelkezik a vizsgáztatott témakört illetően. Vizsgák esetében a feleletválasztós és kifejtős (esszé) típusú kérdések jellemzők. Előbbieknél lehet nehezíteni a vizsga szintjét, ha nem ránézésre egyértelmű válaszokat adunk meg, illetve a válaszok struktúrája, tartalma esetén több válasz is jónak tűnik, de a kérdés a „melyik válasz a legjobb/a legvalószínűbb/a legkevésbé jó", vagy „Több jó megoldás is van!" fordulatokkal operál. Esszékérdéseknél fontos, hogy a hallgatók a saját szavaikkal fogalmazzák meg a válaszokat. Fontos, hogy legyen egy egyértelmű szempontrendszer, amivel mérni tudjuk, hogy a folyószöveges válaszban szerepel-e minden lényeges elem, ami az adott téma esetén igazolja, hogy a hallgató megfelelően felkészült.

Több csoportos vizsgakérdéssor létrehozása azért lehet fontos, mert – főleg tantermi oktatások vizsgája esetén – jellemző, hogy a hallgatók renitensek, és megpróbálnak lesni vagy kommunikálni egymással. Amennyiben több vizsgakérdéssort alkalmazunk, az ilyenfajta nem megengedett kooperáció valószínűsége csökkenthető. Fontos, hogy az egyes kérdéssorok ugyanazokat a témákat dolgozzák fel és a kérdésekre adott válaszokból egyenlő mértékben lehessen a vizsgáztatott tudásszintjéről meggyőződni.

Olyan képzéseken, ahol nem elegendő egy tesztsor kitöltése, ott a tudást a gyakorlatban is tudni kell alkalmazni. Ennek szintén több féle szintje és módszere van, erről az *Incidenskezelési gyakorlatok típusai* című részben esik szó bővebben.

7.1.5. Az incidenskezelés folyamata és szakaszai

A végfelhasználók különösen nagy értéket képviselnek az incidenskezelést végző csoport vagy szervezet számára az incidenskezelés folyamatában. Ugyanakkor hatalmas felelősséggel is bírnak. Kritikus szerepük van azáltal, hogy ők, a végfelhasználók az elsők, akik általában valamilyen incidens jelével először találkoznak. Gondolhatunk itt egy alkalmazás nem megszokott működésére, egy gyanús csa-

tolmány beérkezésére az e-mail-postafiókba, egy gyanús telefonhívásra, egy elhagyott pendrive-ra, ami az irodában a folyosón hever. A felhasználók azon képessége, hogy időben felismerjék a fenyegetéseket, és a megfelelő kockázati attitűddel felmérjék a valós veszélyt, és időben jelezzék azt az incidensmenedzsmenttel foglalkozó szervezet számára, létfontosságú.

Nem szabad elfeledkezni arról sem, hogy egy biztonsági incidensnek milyen gazdasági hatásai lehetnek. A nem képzett felhasználók miatt a szervezetnek számos incidenst kell elszenvednie. Ilyenek minden szervezetben vannak, esetleg nem ismerik fel vagy nem mérik és nem tartják nyilván őket. Egy incidensnek számos ponton lehet gazdasági hatása, kezdve az esetleges üzleti működés megszakadásából fakadó bevételkieséstől, az incidens elhárításához és kivizsgálásához szükséges túlórák elrendelésén és a szakértők felfogadásán, a büntetések kifizetésén át a javító folyamatokig és az újonnan felmerülő beruházásokig sok mindenre kiterjedhet. Vannak olyan károk és hatások, amelyek pedig nem, vagy nagyon nehezen számszerűsíthetők. Ennek a fejezetnek a célja bemutatni, mi a feladata a felhasználónak az incidensek előtt, alatt és után. Egyes módszertanok ezen hármas felosztásnál részletesebben kategorizálják a tevékenységeket, a lényeg azonban nem változik.

7.1.5.1. Végfelhasználói feladatok az incidens előtt

Amikor egy szervezet szeretne felkészülni a hatékony incidenskezelésre, mindenekelőtt azt kell szem előtt tartania, hogy senki nem tökéletes. Sőt, garantáltan mindeki követhet el hibákat, adott esetben a legjobban kiképzett felhasználó vagy üzemeltető is. Az incidensek jelentős része a felhasználóktól eredeztethető.

Ilyen tipikus hibák lehetnek (a felhasználó otthoni és munkahelyi munkaállomását és okoseszközét is figyelembe véve):

- a vírusvédelem kikapcsolása, használatának mellőzése;
- a vírusszignatúrák frissítésének mellőzése;
- az ismeretlen forrásból származó e-mailek és csatolmányaik megnyitása;
- a nem jogtiszta (feltört) programok használata, és az ezzel járó vírusfertőzések kockázatának figyelmen kívül hagyása;
- a felhasználó gépén, telefonján lévő programok frissítésének elmulasztása;
- az adatmentések elmulasztása;
- a publikus hálózatokon, nem titkosított csatornán a privát jelszavak megadása;
- könnyen kitalálható, megtippelhető jelszavak használata, ráadásul több helyen beállítva ugyanaz a jelszó;
- a túlzott jogosultságokat kérő alkalmazások használata.

A fentiek elkerülése érdekében az első és legfontosabb feladat, hogy megfelelően kiképezzük a felhasználókat, akiknek az incidens előtti feladataik az alábbi felsorolásban találhatók:

- részt kell venni az információbiztonsági és IT biztonsági oktatásokon;
- aktívan részt kell venni a biztonságtudatossági kampányokban, nyomon kell követni a témákat és aktualitásokat;
- meg kell tanulni felismerni a szervezetet és a felhasználókat érintő, jellemző fenyegetéseket és potenciális incidenseket (adathalászat, kártevőt terjesztő e-mailek és weboldalak, social engineering, besurranó tolvajok stb.);
- meg kell ismerni és meg kell tanulni az alap kontrollokat (jelszókezelés és -választás, adathordozó kezelés, adatkezelés és -továbbítás, mentések, fizikai biztonsági szabályok, belépőkártya használata, ismeretlen személyek megkérdezése stb.);
- meg kell tanulni, hogy egy biztonsági incidensnél mi a felhasználó szerepe;

- és talán a legfontosabb: a biztonsági incidensek és ezek gyanúja esetén a jelentési csatornák ismeretének és használatának elsajátítása (HelpDesk, abuse@ e-mail cím, Intraneten bejelentő kitöltése, fontos telefonszámok).

Maga az oktatás és a képzés, a biztonságtudatossági kampányok összköltségükben elenyészők a többi információbiztonsági technológiához és kontrollhoz képest, ellenben a szervezet számára adott értékük maximális. Egy jól felkészült felhasználó, aki időben felismer egy incidenst, rengeteg pénzt és erőforrást takarít meg a cégnek.

7.1.5.2. Végfelhasználói feladatok az incidens alatt

Egy már folyamatban lévő incidens alatt a legfontosabb, hogy a felhasználó haladéktalanul kapcsolatba lépjen az incidenskezelést végző csoporttal vagy szervezettel. Például, ha egy felhasználó rosszindulatú csatolmányt tartalmazó levelet talált a postafiókjában – amit ezek szerint a szervezet vírusvédelmi rendszere nem szűrt ki –, és erről értesíti a biztonsági területet, ők már ellenőrizni tudják, hogy ettől a feladótól, erről a címről, ezzel a tárggyal és ezzel a csatolmánnyal még hány felhasználó kapott levelet. Ha csak kevesen, akkor személyesen is értesíteni tudják őket (még mielőtt megnyitnák a levelet), ha pedig sokan érintettek, úgy másféle szükséges lépéseket tudnak tenni (például központilag törlik a leveleket). E példából is látszik, mennyire fontos a felismerés és a gyors reagálás mind a felhasználó mind az incidenskezelést végző szervezet oldaláról.

A fenti eset rosszabb forgatókönyve szerint a felhasználó megnyitja a levelet és a csatolmányt, sőt többször rákattint, elvégre látszólag nem történt semmi, holott a kártevő már töltötte le a futtatható állományt a háttérben, majd még tovább is küldte a levelet a belső címekre a kollégáknak, hogy nézzék meg ők is, mert neki nem nyílik meg rendesen a csatolmány. Ebben az esetben a felhasználó nem ismerte fel a veszélyt, sőt segített a támadóknak még több felhasználóhoz eljuttatni a kártevőt.

Hogy az ilyen eseteket elkerüljük, a felhasználónak incidens során az alábbi feladatai vannak:

- hálózatbiztonsági incidens esetén a legszükségesebbre kell korlátozni a hálózati kommunikációt;
- incidens esetén nem hősködni kell, vagy egyedül megpróbálni megoldani a helyzetet, és saját felelősségre nem szabad nyomozati tevékenységet sem végezni;
- incidens esetén nem szabad új folyamatokat és alkalmazásokat kipróbálni/tesztelni (például a kollégákat megkérni, hogy próbálkozzanak ők is);
- minden változást, anomáliát, nem megszokott működést, gyanús viselkedést (ember és program vagy hálózat által végzettet egyaránt) meg kell próbálni naplózni, a dátum és a minél részletesebb idő megjelölésével, és időben jelenteni kell az incidenskezelést végző csoportnak vagy szervezetnek;
- abban az esetben, ha a felhasználó felelős a vírusvédelmi szignatúrák, illetve a munkaállomáson/gépen/telefonon lévő programok frissességéért, és azok elavultak, úgy haladéktalanul le kell tölteni, valamint tesztelni és telepíteni a legfrissebb verziókat;
- amennyiben fizikai biztonságot érintő incidens van, követni kell a vonatkozó szabályokat, illetve a feljogosított személyek által adott instrukciókat;
- fontos, hogy a felhasználó az incidens folyamatában együttműködjön az incidenskezelést végző csoporttal vagy szervezettel, ne hátráltassa a munkájukat;
- incidens esetén az incidenskezelést végző csoportnak vagy szervezetnek olyan jogosítványai is lehetnek, amelyekkel adott esetben szervezeti hierarchiában magasabban lévőknek is adhatnak utasítást, korlátozhatnak és/vagy tilthatnak tevékenységeket. Természetesen ezeket a jogosítványokat nem ad hoc jelleggel szerzik meg, hanem az incidensmenedzsment folyamatai és szabályai szerint, s annyi időre rendelkeznek ezekkel, amennyire minimálisan szükséges.

7.1.5.3. Végfelhasználói feladatok az incidens után

Az incidens addig tart, amíg az incidensmenedzsmentért felelős csoport vagy szervezet lezártnak nem nyilvánítja azt. Ezt követően kerülnek sorra az incidens utáni feladatok, amelyek a következők a végfelhasználók számára:

- ha vannak olyan események vagy körülmények, amelyeket az incidens alatt nem sikerült rögzíteni és dokumentálni, mindezt utólag kell pótolni;
- a meglévő folyamatok és eljárások javításához információkat kell szolgáltatni (lessons learned);
- amennyiben résztvevőként bevonják a felhasználókat az incidenskezelési folyamatok és szabályzatok javításába, abban hatékonyan és konstruktívan kell részt venni;
- visszajelzést kell adni az incidenskezelési csoportnak vagy szervezetnek, hogy felhasználói oldalról mennyire volt érthető, kezelhető az ő működésük;
- az incidenskezelési csoporttól vagy szervezettől és egyéb résztvevőktől érkező visszajelzéseket meg kell hallgatni és meg kell fontolni;
- amennyiben az incidenst lezáró riport alapján új szabályokat és folyamatokat hirdetnek ki, ezen új ismereteket el kell sajátítani, részt kell venni az ezekről szóló oktatásokon.

7.1.5.4. Az incidenskommunikáció és az incidensjelentési csatornák

A felhasználó legfőbb felelőssége, hogy időben értesítse az incidenskezeléssel foglalkozó csoportot vagy szervezetet. Nagyon fontos, hogy a szervezet egyértelműen kijelölje azon csatornákat, amelyeken incidensbejelentéseket fogad.

Még ahol nincs 7x24 órás incidensmenedzsment-eljárásrend kialakítva, ott is kell olyan csatornákat biztosítani, melyeken bárki be tud jelenteni egy észlelt incidenst. Ilyen esetben nem feltétlen szükséges, hogy rögtön az incidenskezeléssel foglalkozó csoporthoz vagy szervezethez érkezzen a bejelentés, elég például egy telefonos ügyfélszolgáltat, vagy IT HelpDesk, akik aztán majd az előzetes szempontrendszer alapján eldöntik, szükséges-e további eszkaláció, vagy elegendő a normál munkarend szerint értesíteni a szakterületet.

Fontos, hogy a szervezet ne csak a saját munkavállalói számára tegye elérhetővé az incidensbejelentés lehetőségét, hanem biztosítsa, hogy bárki a világon legalább egy csatornán tudjon incidenst, incidensgyanút vagy visszaélést bejelenteni.

Ennek a nemzetközileg elfogadott gyakorlata az úgynevezett abuse@ kezdetű e-mail-cím működtetése. Ennek üzemeltetése rendkívül hasznos, hiszen például egy adathalászat esetén nem kell a mi időzónánkban élő felhasználók vagy ügyfelek reagálására várnunk, hiszen lehet, hogy a világban már órákkal korábban észlelték a támadást, és az abuse@ e-mail-címen már jelezték is. Ha tehetjük, a domainregisztrátornál is tüntessük fel az adatok között az abuse@sajatszervezet.hu címet. Ha valaki informatikai vonalon kapcsolatba szeretne lépni velünk vagy szervezetünkkel, itt meg fogja találni a szükséges kapcsolati adatokat. Az abuse@ e-mail-címet praktikus a honlapon is megjeleníteni.

Ezen kívül még számos csatornát a felhasználók rendelkezésére bocsáthatunk, legyen az Intranetes bejelentő form, incidensbejelentő e-mail vagy telefonszám, illetve jó, ha biztosítunk olyan felületet is, ahol névtelen bejelentést lehet tenni. Ezt a szervezetek nem elsősorban információbiztonsági incidensek, hanem egyéb visszaélés, megvesztegetés, csalás bejelentésére szokták használni, ugyanakkor nem zárható ki, hogy összefüggés áll fenn két jelenség között.

Azt is meg kell tanítani a felhasználóknak, mi az a minimum információhalmaz, amit egy bejelentésnél az incidenskezelő csoport vagy szervezet számára át kell adia:

- a bejelentő neve, szervezeti egysége, elérhetősége;
- az észlelt incidens vagy gyanú leírása;
- képernyőkép vagy egyéb evidencia csatolása;
- amennyiben van, úgy információ az érintett rendszerek és adatok köréről vagy egyéb károkról;

- az esemény feltételezett időpontja – minél pontosabban meghatározva;
- az esemény felfedezésének időpontja (jellemzően nem esik egybe a kettő);
- a már megtett kockázatcsökkentő intézkedések.

Amennyiben a szervezet az incidensmenedzsment folyamatában olyan szintre jutott, készíthet külön bejelentő formot a főbb incidens típusokra.

7.1.6. Incidenskezelési tervek

Ahhoz, hogy incidenskezelési gyakorlatokat lehessen tartani, elengedhetetlen, hogy a szervezet rendelkezzen azokkal az előfeltételekkel, amelyek megteremtik a hatékony incidenskezelés kereteit.

7.1.6.1. Incidenskezelési gyakorlatok

Az incidenskezelés hatékony végrehajtásának biztosítása érdekében a különböző incidenskezelési terveket rendszeresen tesztelni kell. Ez egyszerre szolgálja a kialakított tervek használhatóságának vizsgálatát éles (vagy közel éles) üzleti környezetben, és a résztvevők ismereteinek bővítését, az incidenskezeléssel kapcsolatban az oktatás során szerzett ismeretek felidézését.

A tesztek gyakorisága nagymértékben függ az adott potenciális incidens és a bekövetkezés esetén veszélyeztetett vagyonelemek, adatok vagy támogatott folyamatok fontosságától, a incidenskezelési tervek számától, és az előző tesztek (vagy a bevezetés) óta eltelt időben végrehajtott változtatásoktól.

7.1.6.2. Az incidenskezelési gyakorlatok tervezése

Az incidenskezelési gyakorlatokat előre meg kell tervezni. A tervek elkészítése, azaz a tesztmenetrend kidolgozása annak a szervezeti egységnek a feladata, amely az adott incidenstípus kezelésében a szervezeti feladat, felelősség és hatáskör szempontjából a leginkább érintett.

Egy fizikai biztonsággal összefüggő incidens kezelési gyakorlatát a fizikai biztonságért felelős szervezetnek kell megterveznie, koordinálnia és levezényelnie. Például tűzriadó gyakorlatozása során – ami egy tipikus példája a felhasználókat is érintő incidenseknek – a létesítményüzemeltetés és a fizikai biztonságért felelős terület dolgozik össze, de jellemzően utóbbi a kijelölt vezető.

Az információbiztonsági incidensek kezelési gyakorlata során az információvédelmi terület a vezető, együttműködve a többi, az incidenskezelési tervben meghatározott területtel, például az informatikai üzemeltetéssel, PR-ral, a humánerőforrás-kezeléssel.

7.1.6.3. Az incidenskezelési gyakorlatok típusai

A szervezetek működésének sajátosságai, valamint idő- és erőforrásszűke miatt nem minden esetben van lehetőség teljes, mindenre kiterjedő tesztelés végrehajtására egy-egy incidenssel kapcsolatban. Emiatt a szervezetek különböző komplexitású tesztek végrehajtására kényszerülnek. A tesztek esetében fordítottan arányos a ráfordítás mértéke a hatékonysággal és a valóságoshoz közeli tapasztalatok megszerzésével.

Szóbeli tesztelés

Az incidenskezelési gyakorlat vezetője a résztvevőkkel előzetesen egyeztetve tűzi ki a szóbeli teszt időpontját és helyszínét, valamint az érintettek körét. Szóbeli tesztelés nem igényel nagyfokú erőforrás-ráfordítást, szervezést és előkészítést, azonban az eredményeket is ennek fényében kell figyelembe venni és értékelni.

Egy fiktív incidenshelyzetet szimulálva a résztvevők szóban kifejtik feladatukat a következő szempontok figyelembe vételével:

- feladatszegmensek;
- input/output adatok, dokumentumok;
- értesítési utak, módok, kontaktszemélyek;
- adattárolás, rögzítés, iktatás;
- rendszerek mentése visszaállítása.

A hozzászólások a feladatok funkcionális egymásra épülésének sorrendjében követik egymást.

Helyzetszimulációs tesztelés

A helyzetszimulációs teszt esetén a teszt időpontját csak azon felsővezetők tudhatják, akikhez az érintett szervezeti egységek tartoznak. A teszt forgatókönyvét, részleteit, időbeli kiterjedését és erőforrásigényét előzetesen egyeztetni kell velük, hogy a valós üzlet- illetve ügymenetre a tesztelés ne legyen hatással.

A helyzetszimulációs tesztelés már igényel némi előkészületet. Elsősorban tervezési feladatok szükségesek, valamint annak végiggondolása, hogy a teszt milyen hatással lehet az éles rendszerekre és folyamatokra. Akkor jó a szervezés, ha az imént említettekre semmilyen közvetlen hatással nincs, ami pedig nem a tesztelés eredményéből levont következtetések és javító intézkedések hiányát jelenti, melyek inkább tudatos(ított) eredményei és előzetesen mozgatórugói az egész tesztelésnek.

A teszt során az incidenskezelés által érintett valamennyi folyamatot és fő lefutási ágat szimulálni kell. Az incidenskezelés során a folyamat valamennyi lépését végre kell hajtani, többek között tehát a naplóállományok kiértékelését, a vezetők tájékoztatását stb.

Komplex tesztelési gyakorlat

A komplex tesztelési gyakorlat, ahogy a neve is mutatja, a legbonyolultabb; a legtöbb szervezést és egyeztetést ez igényli.

Ennél a gyakorlattípusnál a lebonyolításnak helyet adó szervezet mint házigazda gondoskodik arról, hogy az előzetesen egyeztetett incidens-forgatókönyvekhez szükséges informatikai rendszerek – tesztrendszerek, vagy a valós, éles környezettel megegyező konfigurációjú, de éles adatokat nem tartalmazó rendszerek –, kommunikációs csatornák, üzemeltetők és minden olyan szereplő rendelkezésre álljon, amelyek egy éles incidens kapcsán érintett lehetnek.

A tesztrendszer lehet egy szervezet leegyszerűsített, az éles környezetektől fizikailag leválasztott rendszere, a megfelelő határvédelmi, végpontvédelmi eszközökkel, valamint egyéb védelmi rendszerekkel, mint például naplóelemző rendszer, APT, és DLP.

Komplex tesztelési gyakorlat esetén valós támadás történik a tesztrendszer ellen, és ez váltja ki az incidenskezelésben érintett szervezetek reakcióit, amelyek lehetnek szimuláltak vagy valósak (például támadásjelzés egy CERT felé, kommunikáció a hatóságokkal és felügyeleti szervekkel). Ilyenkor fontos, hogy a valós kommunikáció valós válaszokat, reakcióidőket váltson ki. Ez, ha az incidenskezelésben érintett szervezetek és folyamatok nincsenek megfelelően kialakítva, akár sok ideig is eltarthat,

ezért a tesztelés szervezőjének fel kell készülnie a tesztelési tervben ilyen esetekre is. Természetesen mindent dokumentálni kell, és a tesztelés végén ki kell elemezni a tapasztaltakat.

7.1.6.4. A tesztelés lebonyolítása

Bármelyik tesztelés végrehajtását is választja a szervezet, az alábbi fő lépéseket minden esetben követni kell.

- Tesztelési forgatókönyv elkészítése;
- a szükséges jóváhagyások beszerzése;
- a kötelezően értesítendők értesítése;
- a teszt végrehajtásához gondoskodni kell a megfelelő helyiség(ek)ről, továbbá a résztvevők ellátásáról, mivel egy-egy tesztelés akár egész nap vagy több napig is eltarthat;
- a résztvevők és a helyettesek listázása;
- komplex tesztelés esetén a tesztrendszerek, a kommunikációs vonalak előzetes ellenőrzése;
- a tesztelési forgatókönyv(ek) végrehajtása;
- a tesztelés folyamatos vagy késleltetett dokumentálása, a bizonyítékok begyűjtése;
- a teszt kiértékelése, a tanulságok levonása, a javaslatok összegyűjtése a javító intézkedések végrehajtására;
- a javító intézkedések végrehajtása.

Az időtartam

A tesztelés időtartamát befolyásolja a tesztelni kívánt feladat komplexitása, az egymásra épülő feladatszegmensek, valamint a tesztelésben résztvevők, egyének, csoportok, illetve szakterületek száma. Fontos tényező a tesztelendő intézkedések kidolgozottsága, vagyis a tesztelés mélysége. A hatásokat célszerű legalább két-három szintig vizsgálni, hogy láthatóvá váljon a továbbgyűrűzésük mértéke. Ugyancsak az időtartamot befolyásolja a lebonyolítás gördülékenysége, illetve – amennyiben olyan a tesztelés – a tesztciklusok száma.

A résztvevők

Az incidenskezelési teszteken minden érintett szervezeti egységtől legalább egy munkatársnak javasolt részt vennie, aki a tesztelni kívánt folyamat aktív résztvevője (A tovagyűrűző hatások által érintett szervezeti egységek képviselőit is hasznos lehet elhívni.) Fontos résztvevő az érintett informatikai rendszer üzemeltetéséért felelős terület, amelyet, ha külsős az üzemeltető, az üzemeltetést végző cég munkatársai képviselnek, akik kapcsolatban állnak a tesztelni kívánt folyamatot támogató informatikai alkalmazással. Jelen kell lennie a tesztelés során egy jegyzőkönyvvezetőnek, a lebonyolítónak, a felső vezetés egy delegált tagjának, valamint külső és független szakértő(k)nek. Fontos résztvevők a hatóságok és felügyeleti szervek képviselői. Amennyiben igény van rá, egyéb megfigyelőket is meg lehet hívni.

Egyéb szempontok

A tesztelés lebonyolítása során minden résztvevőnek arra kell törekednie, hogy ne maradjanak homályos, nem kellőképpen tisztázott részek. A tesztelés lebonyolítója futtassa végig ismételten a kérdéses folyamatot, ha tisztázatlan szerepeket vagy feladatokat tapasztal a teszt lefolytatása során.

7.1.6.5. A teszt kiértékelése (lessons learned)

Az incidenskezelési teszt befejeztével, még a tesztelés részeként, a résztvevőknek ki kell értékelniük azt. A lebonyolító és a tesztelés felelőse a funkcionális vezetőkkel közösen feljegyzést készít a tapasztalatokról, a következő tényezőket figyelembe véve:

- az incidens elhárítására tett intézkedések a meghatározott időn belül megtörténnek-e?
- Az incidenskezelési tervben előre meghatározott funkciók, informatikai rendszerek, kapcsolattartók, kommunikációs vonalak, reakciók az előre meghatározottak szerint, az előre definiált időn belül rendelkezésre álltak-e?
- Amennyiben az egyes funkciók vagy reakcióidők előzetesen SLA-kban (Service Level Agreement) le voltak fektetve, megfeleltek-e az ott rögzített paramétereknek?
- Mennyire volt folyamatos a tevékenység, voltak-e szakadási pontok, volt-e olyan, hogy az incidenskezelés vagy a későbbi lépések elakadtak, vakvágányra futottak? Ha igen, ennek okát mindenképpen fel kell tárni, hiszen ezek fogják a javító intézkedések alapját képezni.
- Az információáramlás, feladatdelegálás megfelelően zajlott-e?
- Voltak-e az incidenskezelési tervben olyan pontok, amelyek megfogalmazása, ennek következtében az ellátandó feladat vagy funkció nem volt egyértelmű?

A kiértékelés és az eredmények teljeskörűsége érdekében célszerű begyűjteni az elsősorban megfigyelési céllal jelenlévő személyek, szervezeti képviselők észrevételeit is (a későbbi felhasználhatóság céljából inkább írásos formában). Sokszor a külső szemlélők objektívebben látnak bizonyos dolgokat, mint azok, akik operatívan részt vesznek egy folyamatban vagy cselekményben.

7.2. Az incidenskezelés bemutatása a tudatossági oktatásokban

Annak érdekében, hogy a felhasználók biztonságtudatossága és kockázatérzékenysége megfelelő szinten legyen, a szervezetnek komoly erőfeszítéseket kell tennie. Nem elegendő a téma fontosságára egyszer egy évben felhívni a figyelmet. A szervezetet folyamatosan érik különféle támadások, ezért állandó szinten tartás szükséges.

A biztonságtudatossághoz elengedhetetlenül hozzátartozik a *kockázatérzékenység,* ami egy fluidum, kézzelfoghatatlan és pontos definíciókkal nehezen körülírható fogalom. Ez a tudatosítható és fejleszthető készség végső soron megóvja a végfelhasználókat és ezáltal a szervezetet is a biztonsági incidensektől és azok következményeitől.

Sajnos a tudatosság és a kockázatérzékenység nem állandó tudatállapot, rengeteg minden befolyásolja: egyebek mellett a felhasználó terheltsége, stresszes vagy éppen rosszkedvű hangulata. Ilyen esetekben a tudatossági szint romlik, adott esetben olyan tevékenységeket is végrehajt a felhasználó, amit normális esetben, nyugodt körülmények között nem, ezáltal pedig nagyobb kockázatot vállal, ami hatással lehet akár az adott nem kívánt esemény bekövetkezési valószínűségének növekedésére, akár a bekövetkezéssel okozott kár nagyságára.

Ezen esetek megmagyarázása kezdődik az „azt hittem”, „úgy tudtam”, „elfelejtettem” frázisokkal. Mindhárom arra vezethető vissza, hogy a felhasználónak nem volt elegendő vagy megfelelő ismerete, gyakorlata, vagy a kockázatérzékenysége volt nagyon alacsony, emiatt rossz döntéseket hozott, melyekből később vagy azonnal biztonsági incidens keletkezett.

7.2.1. A biztonsági oktatások és a tudatossági kampányok végrehajtásának előnyei

A végfelhasználói és szerepkörönkénti biztonsági oktatásoknak és a tudatossági kampányoknak az eredeti céljaikon túl további hozzáadott értékeik is vannak a szervezetben. Az oktatásokat követően,

amennyiben a felhasználók a gyakorlatban is alkalmazzák a hallottakat, csökkenni fog a szervezet kockázati szintje. Kialakul a felhasználókban egy „egészséges paranoia”: ha a jövőben számukra ismeretlen jelenséggel vagy viselkedéssel találják szemben magukat, eleve fenntartással fogják kezelni azt, esetleg arról mint incidensgyanúról bejelentést is tesznek. A felhasználók, mivel különbséget fognak tudni tenni *hiba* és *fenyegetés* között, hatékonyabban fogják végezni munkájukat, illetve olyan gyengeségeket, hibás működéseket, szabályozási pontatlanságokat is jelezni fognak, amelyek által javíthatók a folyamatok, fejleszthetők az informatikai rendszerek.

A biztonságtudatossági kampányok által – melyeken a biztonsági területeknek lehetőségük van bemutatkozni – növekedni fog a területek ismertsége és népszerűsége. Ez egy nagyon fontos dolog, mert sokszor a felhasználók az információvédelmet és általában a biztonságot valamiféle fekete mágiaként vagy „Big Brother”-ként kezelik, a biztonsági szakértőket fura alakoknak tartják, ezáltal azt az elvet vallják, hogy inkább nem szólnak semmiről, és abból nem lehet baj. Ez nagyon rossz hozzáállás, és a kampányokat ki kell használni arra, hogy a szervezet bemutassa, hogy az információbiztonsági felelős vagy szakértő is ember, ugyanúgy él, dolgozik, vannak feladatai, problémái, és meg lehet őt szólítani, meg lehet keresni akár olyan problémával is, amely a felhasználók privát információvédelmi kérdéskörébe tartozik. Ha a szervezet megismeri a biztonsági területeket, sokkal kevesebb ellenállást fog kifejteni egyes intézkedések kapcsán, illetve a felhasználók fognak kérdezni, kialakul egy egészséges párbeszéd.

7.2.2. Eszközök a munkavállalók figyelmének felkeltésére, fenntartására; motiváció, buy-in, lessons learned

A munkavállalók figyelméért számos szervezeti egység versenyez. A munkavállalók figyelme megosztott, ők elsősorban azon tevékenységekre koncentrálnak, amelyek az alaptevékenységükhöz kapcsolódnak, amiért a fizetésüket kapják. Ezért is fontos, hogy a biztonságot és az információvédelmet érintő feladatok és felelősségek megjelenjenek a munkavállalók munkaköri leírásaiban, munkaszerződéseiben, illetve ugyanígy megjelenjenek a szervezet minden olyan szerződésében, amelyben a szervezet adataihoz, információhoz, rendszereihez vagy egyéb eszközeihez fér hozzá külsős.

Ugyanakkor – legyünk őszinték – az, hogy a munkaköri leírásban szerepel valami, még kevés ahhoz, hogy folyamatosan a felhasználó figyelmének fókuszában legyen, és aktívan hasson a napi tevékenységre, esetleg pozitív irányba befolyásolja a biztonságtudatosságot és kockázatérzékenységet.

A biztonsággal, biztonságtudatossággal, információvédelemmel kapcsolatban ugyanazokat a figyelemfelhívó eszközöket kell használni, mint minden más olyan téma kapcsán, amelyeket a végfelhasználóknak szem előtt kell tartaniuk.

A biztonságot „el kell tudni adni”, mint egy terméket. Általában, ha egy szervezet nem a világtól elszigetelve próbál működni, jelen vannak azon szervezeti egységek, amelyeknek az a szakmájuk, hogy a szervezettel kapcsolatos információkat kommunikálják, a szervezet termékeinek és szolgáltatásainak értékesítésében és reklámozásában részt vegyenek. Maga az a folyamat, ahogy a végfelhasználókat megszólítjuk és elérjük, ugyanaz, mint amikor egy szervezet promotálja a termékeit.

A biztonságtudatosság és kockázatérzékenység kialakításához tananyagokat kell készíteni, oktatásokat kell tartani, cikkeket és hírleveleket kell készíteni és eljuttatni a felhasználókhoz, és általában minden PR- és médiacsatornát, valamint marketingeszközt fel lehet és fel kell használni az üzenetek célba juttatására.

Mindenki elfoglalt. Az embereknek a biztonság és az információvédelem sokszor nyűg, ezért olyan eszközöket kell bevetni, amelyek elérik az ingerküszöbüket, olyan marketingeszközöket kell használni, amelyek színesek, érdekesek, felkeltik a figyelmet. De ez még csak az egyik része a dolognak, mert fent is kell tartani a figyelmet, mivel általában sok mondanivaló fogalmazódik meg egy-egy biztonságtudatossági kampányban vagy oktatási anyagban.

Ha nincs meg a motiváció, akkor az a rengeteg energia, amit beleöltünk egy tudatossági kampányba, elvész. Ezért a tudásátadás minden egyes szakaszát meg kell tervezni, mert ha a folyamatban valahol lankad a motiváció, az egész folyamat elveszíti az értékét, és a felhasználók továbbra is a saját fejük után fognak menni.

A felhasználókban tudatosíttatni kell saját szerepüket az egész információvédelemben, incidenskezelésben. Lessons learned: célszerű a biztonsági incidensek után közreadni olyan esettanulmányokat, amelyek a szervezet saját életéből valók. Ezekben ki lehet térni a felismert és időben megelőzött incidensekre is, valamint a megtörténtekre is, megmutatva, hogy mik voltak a kritikus pontok, a jó és rossz gyakorlatok.

7.2.3. A tudatosságépítés folyamata, motivációk, figyelemfenntartás

A tudatosságépítés az alábbi fő folyamatlépésekre bontható. Az oktatásokkal, vizsgákkal, kampányokkal, az incidenskezelési gyakorlatokkal a felhasználókat ezeken a stációkon kell keresztülvezetni:

5. ábra

A biztonságtudatosság kialakításának folyamata

Forrás: A szerző saját szerkesztése

7.2.4. A biztonsági oktatás és a tudatossági kampány közti különbségek

Az oktatás egyre nagyobb hangsúlyt kap a szervezetek életében, azonban a hatékonysága sokszor erősen megkérdőjelezhető. Sok esetben kötelező nyűgnek tartják: a lényeg, hogy a jelenléti ívet aláírva be lehessen mutatni az auditornak.

Azon szervezetek, akik ezt a gyakorlatot követik, a legolcsóbb és leghatékonyabb biztonsági kontrolljukról mondanak le.

Érdemes a száraz szervezeti szabályok puszta átadása mellett a végfelhasználóknak azt is megmutatni, hogy e szabályok betartásával a saját életükben is rengeteg problémától, adatvesztéstől, lopástól, pénzügyi veszteségtől és egyéb kellemetlenségtől kímélhetik meg magukat. Ha a felhasználók tudatosítják, hogy nekik és a szervezetüknek is vannak fontos adataik, s ugyanolyan informatikai eszközöket használnak, könnyebben belátják, hogy ugyanúgy fenyegetik őket is különböző dolgok az internet felől vagy a való életben, mint a céget. Így sokkal könnyebb a szervezeti biztonsági szabályokat is elfogadtatni velük. Egy-egy szabály vagy biztonsági kontroll bevezetése egyszerűbb lesz, mivel kisebb személyes ellenállásba fog ütközni; lesznek saját példák és élmények, amelyekkel már közel is hoztuk a sokszor megfoghatatlan dolgokat a felhasználókhoz.

A felhasználók saját értékeik, adataik, rendszereik, környezetük biztonsági fenyegetettségei és kontrolljai bemutatása által megnyerhetők a szervezet biztonsági céljainak elérésére. Ennek eszköze a tudatossági kampány, ami bár tartalmazhat szervezetspecifikus információkat és témákat is, alapvetően a felhasználóról és az ő mindennapi életéről kell, hogy szóljon.

7.2.5. A biztonságtudatossági kampányok tervezése, előkészítése és végrehajtása

Ha a szervezet úgy dönt, hogy biztonságtudatossági kampányt szeretne megvalósítani, azt már a megelőző évben pénzügyi oldalról is tervezni kell. Ha adott évben nincs elkülönítve pénz, akkor a szervezet életében bejáratott módszerrel – egyedi előterjesztés, átcsoportosítás stb. – kell a megfelelő pénzösszeget előteremteni. Ezután következhet a szakmai tartalom megtervezése, majd a megvalósítás és a visszamérés.

7.2.5.1. A biztonságtudatossági kampány emberi erőforrásigénye

Egy kampány megszervezése körülbelül két-három hónapnyi szakértői munka. A kiválasztott szakember felelős többek között a pénzügyi tervezésért, a kapcsolattartásért a társterületekkel, a kampány során végrehajtott aktivitás pontosságáért, a média- és reklámanyagok elkészíttetéséért, a visszamérésért. Ugyanakkor számos társterülettel együtt kell működnie, melyeknek szintén praktikus dedikált felelőst kijelölniük, aki segíti a kampányszervező(k) munkáját.

A marketingért felelős szervezeti egység felelős a marketing eszközök, látványtervek, szóróanyagok megtervezéséért (témakörök alapján). Észben tartandó, hogy egyedi igényekre egyedi árakat fogunk kapni, ami jócskán megdrágíthatja a kampányt. Ugyanennek az egységnek a dolga az imént említett anyagok legyártatása és szállítása, valamint a hostessek szervezése.

A PR/kommunikációs szervezeti egység dolga a tájékoztatási csatornák leegyeztetése, a belső kommunikáció megtervezése és az Intranet felület, a bannerek, az ütemezett hírek, a céges újság és a fotók elkészítése.

A beszerzési terület feladata a normál (marketing és PR) csatornákon kívüli beszerzések intézése (például díjak és ajándékok, plakátkeretek).

Az üzemeltetés (telephelyek és központi épületek egyaránt) felel a szóróanyagok terítéséért, az épületeket érintő tevékenységek egyeztetéséért (liftmatrica, plakátok kihelyezése, leszedése, reklámajándékok kiosztása).

Az IT szervezet dolga például a reggelente a bejelentkezési processz után megjelenő biztonsági tippek IT előkészítése, és a biztonsági kampányhoz kapcsolódó képernyővédők központi terítése.

A kontrolling/számvitel feladata a költségek megfelelő elszámolása, átcsoportosítása, valamint az esetleges díjak, nyeremények adózási kérdéseinek tisztázása.

A fentiekből is látható, hogy a tudatossági kampányszervezés egy komoly és összetett, belső projekt. Elengedhetetlen a vezetői támogatás.

7.2.5.2. A pénzügyi tervezés

A szakmai tervezés költsége

Amennyiben a szervezetnek nincs erőforrása a szakmai tartalom előkészítésére, erre külsős tanácsadó cégeket vehet igénybe, akik az előzetesen kialakított tematikához elkészítik a szakmai anyagokat. Ezek lehetnek cikkek, hírgyűjtemények, esettanulmányok, visszamérő kérdések és válaszok vagy akár egy komplett totójáték is. Ennek a költsége a tematika függvénye. Fontos, hogy ha összefog a szervezet összes biztonsági területe, és a kampány során mindegyik megosztja a saját ötleteit és témáit, és ezek kidolgozása külsősre van bízva, az komolyabb, akár milliós költségtétel is lehet. Ugyanakkor egy belsős dedikált szakértő, aki fel van jogosítva arra, hogy a társterületeket is mozgósítsa a kampányanyagok határidőre és megfelelő minőségben történő elkészítésére, meg tudja oldani mindezt a munkaidejében is.

A marketingköltség

Ez az egyik legnagyobb tétel. Nagyon fontos észben tartani, hogy egy tudatossági kampányban a biztonsági témák gyakorlatilag termékek, amelyek esetében fel kell kelteni és fenn is kell tartani az érdeklődést. Mindehhez gyakorlatilag ugyanazokat az eszközöket kell használni, mintha egy terméket próbálnánk meg értékesíteni. Minden megengedett – a pénztárcánk függvényében. Egy nem túl elrugaszkodott kampányban az alábbi figyelemfelkeltő reklámeszközöket célszerű használni: plakátok, reklámajándékok, matricák, lift- és mosdótükör-matrica, tálcaalátét az étteremben, banner.

Költség szempontjából fontos, hogy legyen a kampánynak egy egyedi arculata, amiről rögtön mindenki tudja, mire is utal. Ennek azonban ára van, sok esetben stockfotókat kell vásárolni, illetve a marketinganyagoknak is komoly költsége lehet a minőségtől, mérettől és darabszámtól függően. Az arculattervezésért a marketingügynökségek komoly összegeket tudnak elkérni. Ezért fontos, hogy ezt a részt bízzuk a marketingért felelős szervezeti egységre.

Motiváció – a játékok díjai (heti és fődíjak)

Noha az embereket alapvetően a téma is érdekli, hosszabb távon – például egy komplex, több biztonsági területet is érintő kampányban – célszerű valamilyen gamification-t, játékot is tervezni. Az emberek szívesen játszanak, és szeretnek nyerni. Játékokkal, totókkal az átadott tudást is vissza lehet mérni. Ahhoz, hogy a felhasználók részt vegyenek folyamatosan a játékokban, valamilyen díja(ka)t célszerű felajánlani. Ezek olyan értékkel kell, hogy bírjanak, amely már megmozgatja az emberek fantáziáját.

Példaként elgondolható egy négy hetes biztonsági kampány, ahol minden héten egy biztonsági terület mutatkozik be. Naponta különféle témák kerülnek terítékre, és minden hét elején visszamérő totót rendeznek heti nyereménnyel, majd a kampány végén egy főnyereményt sorolnak ki. A heti nyeremény lehet például egy internetbiztonsági szoftvercsomag, egy számítógépes újság-előfizetés vagy egyéb tárgynyeremény. Havi kampánylezáró fődíjként fényképezőgépet, wellness hétvégét, értékes numizmatikai érmet stb. ajánlanak fel.

Ezek költsége körülbelül a marketingköltségekével vetekedhet. Fontos, hogy mind a díjak, mind a marketingköltségek általában nem az adott biztonsági terület költségvetéséhez tartoznak majd, ezért időben gondoskodni kell ezek átcsoportosításáról.

7.2.5.3. A szakmai tervezés

A kampány tematikáját ki kell dolgozni, és napi tervet kell készíteni arról, milyen csatornán milyen aktivitás fog történni. A szakmai anyagokat el kell készíteni, jóvá kell hagyatni az érintett vezetőkkel, és gondoskodni kell arról, hogy minden időben a megfelelő helyre kerüljön. Újságcikkek, hírek, heti totókérdések és válaszok, egyéb aktivitások, interjúk a vezetőkkel stb.

Ha a biztonsági területeknek van saját intranetes oldala, célszerű ott megjeleníteni a szakmai tartalmakat, ezáltal odaszoktatva a felhasználókat.

7.2.5.4. Megvalósítás

A kampány során, ha a tervezés megfelelő volt, nincs más teendő, mint a napi szinten megtervezett aktivitást megvalósítani és ellenőrizni. A reggeli biztonsági tippek megjelennek-e? A megfelelő plakátok lettek-e kihelyezve? Elérhető-e a totó az Intraneten? Megfelelően jelenik-e meg a cikk az Intraneten? És így tovább.

7.2.5.5. Visszamérés

A heti totójáték már önmagában egy indikátor, hogy mennyien vesznek részt benne, és mennyi helyes és helytelen válasz érkezik. Továbbá mérni lehet az egyes intranetes cikkek kattintásszámát, népszerűségét, az egyéb csatornákon érkező kérdéseket, illetve konkrét elégedettségi kérdőívet is kilehet töltetni a felhasználókkal.

A visszacsatolás egyik fontos eszköze lehet, ha a kampány lezárásaként a biztonsági területekért felelős felsővezető vagy maga a cégvezető/szervezeti vezető adja át a díjakat, és köszönti a résztvevőket. Erről szintén egy remek cikket lehet a belsős kommunikációs csatornákon, például az intranetes oldalon közzé tenni.

7.2.6. A biztonsági oktatások tervezése, előkészítése és végrehajtása

A biztonsági oktatások során a szervezet saját biztonsági szabályait és folyamatait szeretnénk a felhasználókkal megismertetni. Természetesen lehet biztonságtudatossági elemekkel is színesíteni az oktatásokat, de alapvetően ennek a belső kontrollkörnyezetről kell szólnia. Abban is különbözik a tudatossági kampánytól egy oktatás, hogy ezek jellemzően kötelezők mindenki számára, illetve gyakran vizsgával zárulnak.

Mint az korábban is elhangzott, végfelhasználói oktatásokon ügyelni kell arra, hogy a szükséges és elégséges tudást próbáljuk átadni.

A biztonsági oktatásokat több szempontból is csoportosíthatjuk. Időbeliség szempontjából megkülönböztethetünk új belépőoktatást és ismétlő oktatást.

Időbeliség: új belépő- és frissítő oktatás

A belépőoktatásnál az új felhasználókat kell megismertetni a szervezeti szabályokkal. Sok esetben (rendszerjogosultságok, hozzáférések esetén) célszerű a sikeres oktatást és vizsgát feltételül szabni.

Frissítő oktatásnál a tartalom hasonló, ezt érdemes évente megismételtetni a teljes szervezettel. Nem jó gyakorlat, ha van új belépőoktatás, de nincs frissítő. Az informatika és a biztonság is éves

szinten rengeteget változik. Hatalmas kockázat, ha valaki akár évekig nem kap képzést az új szabályokról vagy az újonnan felismert fenyegetésekről.

Az oktatás módja: tantermi (frontális oktatás) és/vagy elektronikus tananyagok (e-learning)

Kisebb szervezeteknek (tapasztalat alapján maximum 200–300 főig) célszerűbb frontális, tantermi oktatásokat tartani. Az oktató személye és tapasztalata jelentősen hozzá tud járulni a tananyag megértéséhez és befogadásához.

E létszám fölött azonban a tantermi oktatás már gyakorlati és logisztikai problémákat vet fel, és egyszerűen nem éri meg anyagilag sem, mivel az oktatónak – legyen akár külső vagy belső – így több idejébe fog telni az oktatás, amit pedig a szervezetnek munkaidőként ki is kell fizetnie.

Nagyobb szervezeteknél, ahol időben és térben nem lehet a felhasználók csoportját könnyen mozgatni, minden egyéb témájú oktatás szervezése során ugyanazokkal a problémákkal fognak szembesülni, ezért előbb-utóbb bevezetnek majd egy elektronikus oktatási rendszert (LMS – Learning Management System), amely képes elektronikus tananyagok segítségével számos oktatási célt megvalósítani. Ilyen oktatás lehet az információbiztonsági, de más biztonsági tananyag is. Az e-learning-rendszerek képesek mérni a részvételt, végre lehet hajtani a vizsgáztatást, különböző nyilatkoztatásokat és – a széleskörű riporting lehetőségekkel – remek kimutatásokat lehet készíteni. Az oktatási anyagokat összeállíthatja maga az érintett szakterület, vagy készítheti őket külsős szakértő is, a szervezet igényei által.

Az elektronikus és tantermi oktatási anyagokat is rendszeresen frissíteni kell, a hozzájuk tartozó vizsgakérdésekkel együtt.

7.3. Példák az incidenskezelés bemutatására, végfelhasználók számára

7.3.1. Az adathalászat elhárítása

A támadók/csalók már a kétezres évek közepén rájöttek, hogy egyszerűbb az ügyfelektől pénzt szerezni, mint megpróbálni betörni egy bank informatikai rendszerébe. Ez az állítás még ma is így van, dacára annak, hogy megtörtént már az utóbbi eset is. Egy adathalászat végrehajtásához lényegesen kevesebb tudás és beruházás kell, mint egy hosszú időn át előkészített, sokáig rejtve maradó rendszerfeltöréshez. Komplett adathalászati tool-okat lehetett és lehet ma is kapni az internetes fekete piacokon.

7.3.1.1. Az incidens előtti tevékenységek

A kétezres évek közepén Magyarországon számos bank ügyfelét érte adathalász támadás. Éppen ezért minden magyar bank felkészítette a szervezetét az ilyen támadások kezelésére, az érintettek és minden banki dolgozó részt vett oktatásokon, és számos példán át meg lett értetve a banki dolgozókkal, hogy mi a teendő ilyen esetben. Ezen kívül a bankok a weboldalukon is állandó hivatkozásként olyan biztonsági jótanácsokat publikáltak, amelyek segítettek az ügyfeleknek is.

Most az egyik korai adathalász támadás részletesebb leírása következik. Hogy ne kelljen konkrét banknevet említeni, az érintett intézetet hívjuk Piréz Bank Magyarországnak.

Az adathalászatról dióhéjban: ilyen típusú támadás esetén a támadók a valahonnan megvásárolt e-mail-címlistára elküldenek egy olyan levelet, amely jelen esetben a bank logoját tartalmazza (objektumként vagy külső hivatkozásként), és a levélben felszólítják az ügyfeleket, hogy lépjenek be a levélben található hivatkozáson keresztül az internetbanki fiókjukba, és ellenőrizzék a számlaegyenlegüket,

mert valamilyen biztonsági probléma merült fel. Amennyiben ezt megteszik, a támadók megszerzik az adataikat, amelyekkel aztán már ők próbálnak meg belépni a bank valós honlapján keresztül.

A konkrét levél szövege fordítógéppel volt magyarítva, rengeteg félrefordított szóval, amely még az olvasást is megnehezítette. Feladóként hamis egy e-mail-címet adtak meg, amely az info@pirezbank.hu volt. Ennek a későbbiek során lesz jelentősége. Ezen kívül egy franciaországi pékség weboldalát feltörték a támadók, nem töröltek le semmit, nem cserélték le a weboldalt, csak az egyik belsőbb alkönyvtárban elhelyezték a Piréz Bank internetbanki oldalának egy másolatát, pontosabban a kezdőoldalt, ahol a bejelentkezést kellett végrehajtani. Természetesen az oldal SSL-tanúsítvány nélküli volt. Miután ez megvolt, és minden működött, szétküldték a támadók a több millió levelet.

7.3.1.2. Az incidens alatti tevékenységek

Mivel a Piréz Bank minden dolgozója egyben az intézet ügyfele is volt, óhatatlanul kaptak ők is a levélből. A felhasználók éves új belépőképzésben és rendszeres éves biztonsági képzésben is részesültek, így azonnal felismerték, hogy ilyen levelet a bank biztosan nem küld, vagyis az nagy valószínűséggel csalás. Jó jel volt, hogy az ügyfélszolgálatot is elkezdték hívogatni az ügyfelek. Ekkor még az ügyfélszolgálat, a fiókhálózat és a biztonsági terület sem értesült az incidensről, nem voltak érdemi információk. Volt olyan ügyfél is, aki kinyomtatva bevitte a fiókba, és ott mutatta meg a fióki tanácsadó kollégának az adathalász levelet. Mivel az oktatás során kiemelten sok szó esett az incidensek jelentési csatornáiról, a biztonsági területre elkezdtek érkezni a bejelentések.

Az ügyfélszolgálatos kollégák jelezték a vezetőiknek, hogy egyre emelkedett a telefonos és az ugyfelszolg@pirezbank.hu címre érkező bejelentések száma. A vezető kollégák telefonon kezdeményeztek egyeztetést a biztonsági terület vezetőjével. A fiókhálózatból beszkennelve küldték az ügyfél által kinyomtatott adathalász e-mailt az incidensbejelentő e-mail címre (abuse@pirezbank.hu). A banki dolgozók továbbították a levelet ugyanerre a címre.

A biztonsági terület naplóelemző rendszere ekkor már riasztott; az adathalász levél @pirezbank.hu címmel lett szétküldve, és számos levél kézbesíthetetlen volt (nemlétező cím, megtelt postafiók, automatikus válaszok stb.). Mivel az info@pirezbank.hu volt a (hamisított) feladó, ezért ide érkeztek az automatikus válaszok és a válaszlevelek a kézbesítések sikertelenségéről. Ismerve a jelenséget, a biztonsági naplóelemző rendszerben az ilyen úgynevezett visszapattanó e-mailekre külön szabály volt érvényben, így amikor hirtelen megemelkedett ezek száma, tudni lehetett, hogy valaki nagy mennyiségű levelet küldött a bank nevében. Már csak a levelet kellett megszerezni.

A biztonsági terület azonnal elkezdte a különböző csatornákon beérkezett adathalász levelek elemzését.

Meggyőződtek róla, hogy a bank lett behamisítva feladóként, a küldő e-mail-szerver pedig valamelyik ázsiai országban volt. A levél nem tartalmazott ártó szándékú kódot, sem olyan scriptet, amely kártevőt kezdene letölteni a felhasználó gépére. A levélszövegben mutatott hivatkozás „Belépéshez kérem, kattintson az alábbi linkre: Piréz Internet Bank”, valójában a http://onlinebaghett.fr/var/lib/dpkg/lock/pirezbank/login.html oldalra mutatott. Ellenőrizték, hogy nem banki oldalról linkelték-e be a csalók a banki logo-t, mivel ebben az esetben azt ki lehetett cserélni egy figyelmeztető képfájlra – ugyanazon a néven. Ilyen esetben az adathalász levelet megnyitó felhasználó a banki logo helyett egy figyelmeztetést látna, ami rögtön felfedné, hogy csalásról van szó.

A hamis banki weboldalon, bármit ütött is be bejelentkezési adatként az, aki odatévedt, az oldal továbbdobta a felhasználót egy következő oldalra, ahol további adatokat kértek be a támadók.

Mindezek után a szakértők több párhuzamos tevékenységet kezdtek meg az incidenskezelési terv alapján:

- értesítették az érintett üzleti területeket az incidensről (Elektronikus Csatornák Igazgatóság, Fiókhálózati Igazgatóság, PR Igazgatóság, IT Igazgatóság, Ügyvezető Testület, Belső Ellenőrzési Igazgatóság – mint a felügyeleti szervek kapcsolattartója);

- a PR Igazgatósággal közösen az ilyen esetre előkészített sablon tájékoztató szöveget (scriptet) aktualizálták (teendők, mit szabad mondani és mit nem) és elküldték a Fiókhálózati Igazgatóságnak, hogy az küldje szét a fiókhálózatba, valamint az Ügyfélszolgálat részére a telefonos ügyfélkezeléshez;
- szintén a PR Igazgatósággal közösen egy felhívást tettek közzé az Intraneten, a bank többi dolgozójának tájékoztatására, valamint a bank honlapjának kezdőoldalán és az internetbanki bejelentkezési oldalon figyelemfelhívást tettek közzé.
- szintén a PR Igazgatósággal közösen megfogalmaztak egy sajtóközleményt, amiben felhívták az ügyfelek figyelmét az adathalászatra. Ez nem lett rögtön kiküldve, mivel a sajtótájékoztatás rosszul is elsülhet: esetleg valaki félreérti és pánikot kelt, ami mindenképp kerülendő.

További szakértő kollégák ezalatt felvették a kapcsolatot a bejelentéseket tevő banki kollégákkal és ügyfelekkel, hogy juttassák el számukra az eredeti levelet lementve, mivel ebből további információkat lehetett kigyűjteni, illetve össze lehetett hasonlítani, hogy csak egy hamis weboldal van vagy több, vannak-e más levélvariánsok vagy csak egy.

Mindeközben a szakértők egy nem a banki hálózatra kapcsolt számítógépen elemezték a hamis banki weboldalt, hogy nem tartalmaz-e ártó kódot, és hogy milyen adatokat kérnek be a csalók az ügyfelektől. Felvették a kapcsolatot az ügyfélszolgálattal, mivel a weboldalon olyan adatokat is bekértek a támadók (például PIN-kódot), amivel telefonos bankolás szolgáltatását lehetet igénybe venni. Az ügyfélszolgálat számára elrendelték a szigorított azonosítást és hitelesítést, olyan adatokkal, amelyeket csak az ügyfelek ismertek és a támadók nem kérték el a hamis oldalon. Az ügyfélszolgálat részére készült egy kis összefoglaló az adathalászatról, mivel sok olyan ember is megkapta az adathalász e-mailt, akik nem voltak a bank ügyfelei, így nem értették, honnan tudja az intézet az ő címüket stb. – ezt kezelni kellett.

A felhasználók által beküldött e-mailek és a lementett hamis weboldaltartalom archiválva lett. Utóbbit a népszerű webböngészőkben bejelentették mint csaló, ártó szándékú oldal. A banki felhasználóktól és az ügyfelektől is azt kérte a bank, hogy minél több helyen jelezzék a hamis oldalt (böngészők, adathalászattal foglalkozó szervezetek oldalai), hiszen minél többen szólnak, annál előbb fognak a böngészők és keresők reagálni rá, és ha valaki odatéved, akkor már egy figyelmeztetés fogja várni, amely arra szólítja fel, hogy gyorsan navigáljon el onnan. Az adathalász oldalakat gyűjtő weboldalakon (Phistank, APWG – Anti Phishing Working Group) természetesen maguk a szakértők is tettek bejelentéseket az ügyről, s a Cert-Hungary-t is értesítették a hamis oldal létezéséről. A szakértők informálták a Bankszövetség tagbankjait is a támadásról, hogy ők is fel tudjanak készülni, ha történik hasonló eset. A felügyeleti szervek kapcsolattartó szervezeti egységén keresztül értesítették a Pénzügyi Felügyeletet az incidensről és a megtett intézkedésekről. A szakértők ellenőrizték az onlinebaghett.fr domain név tulajdonosát, és felvették vele és a névszolgáltatóval is a kapcsolatot a technikai elérhetőségeken, mind e-mailen, mind telefonon. Jelezték az üzemeltetőnek, hogy a weboldal valószínűleg fel lett törve, egyben kérték, hogy törölje le a hamis weboldalt a szerverről, megakadályozva a további adatlopást. Ezzel együtt az üzemeltetőnek javasolták, hogy kezdje meg a tartalomszolgáltató programjának (CMS – Content Management System) a biztonsági felülvizsgálatát, mert amíg így marad, a támadók visszatérhetnek, és visszatehetik a letörölt hamis banki weboldalt. (Egy másik esetben ez meg is történt, ahol végül a rendszergazda a teljes weboldalát törölte, mert fogalma sem volt róla, hol lehet pontosan a biztonsági rés).

Mindeközben elkezdtek érkezni azon valódi ügyfelek bejelentései, akik bedőltek a csalóknak, és megadták az internetbanki belépési adataikat. Ezen ügyfelek esetében az ügyfélszolgálat intézkedett a megfelelő protokoll szerint, új azonosítót és új kezdőjelszót állított be. (Ebben az időben még nem volt kötelező a bejelentkezési SMS). Továbbá átnézték a bejelentést tevő ügyfelek internetbank-használati kronológiáját, azt keresve, történt-e gyanús tevékenység (betétfeltörés, utalás rögzítés stb.) A bejelentést tevő ügyfelek esetében a biztonsági szakértő kollégák átnézték az ügyfél bejelentkezési adatainak történetét, olyan anomáliák után kutatva, amelyek eltértek a normál ügyfél általi internetbank-használattól.

Tipikusan ilyen, ha mondjuk az ügyfél utolsó 10 belépése a helyi magyar szolgáltató hálózatából történt, ám a legutolsó a Cambalaya Guest Communications (CABGSTMS) hálózatából, ráadásul 10 perccel az utolsó előtti bejelentkezés után. Ebben az esetben nagyon valószínű, hogy a csalók megszerezték az ügyfél bejelentkezési adatait és próbáltak belépni.

Az érintett szervezeti egységek, beleértve a Piréz Bank felső vezetőségét is, újabb tájékoztatást kaptak a megtett intézkedésekről, kiegészítve mindezt azzal az információval, hogy mennyi érintett ügyfél van, illetve van-e tényleges kár, van-e sajtóérdeklődés, mit reagált a Pénzügyi Felügyelet.

A szakértők lejegyezték az incidens alatt megtett intézkedéseket, lehetőleg pontos dátum- és időpont-megjelölésekkel.

Mivel az ügyfelek, a banki szakértői gárda, a francia weboldal üzemeltetői és az összes érintett terület egyaránt gyorsan reagált, az adathalász levél kiküldésétől számított kb. 30. percben már nem volt elérhető a hamis weboldal, illetve az összes fontos csatornán tájékoztatva lettek az ügyfelek az incidensről.

A gyors reagálásnak köszönhetően a címzettek nagy többsége meg sem nyitotta az adathalász levelet, vagy ha igen, már nem jutott el a csaló weboldalra. Mivel nem volt újabb e-mail-variáns és nem volt további hamis weboldal más feltört szerveren, kijelenthető volt, hogy az incidenst sikerült elhárítani.

Ehhez szükséges volt, hogy a felhasználók tudják mivel állnak szemben, ismerjék és alkalmazzák az incidensbejelentési csatornákat. Továbbá, hogy a szakértő területek és az érintett területek rendelkezzenek incidenskezelési tervvel, és tudják használni is azokat. Legyenek előkészített scriptek, sajtóközlemény-vázlatok és incidens specifikus folyamatok. Legyen megfelelő számú szakértő, akik a fenti sok-sok feladatot nem lineárisan, hanem párhuzamosan tudják végezni.

Ha a fenti tevékenységeket egy embernek kellett volna végrehajtania, körülbelül 5–8 óráig tartott volna mindent elvégezni. Addigra sokkal több ügyfél adta volna meg az adatait, emiatt valószínűleg tényleges anyagi kár is keletkezett volna, illetve exponenciálisan nőtt volna az incidensben érintett ügyfelek tevékenységének és logjainak az elemzésére fordítandó idő. Erősen sérült volna a bank reputációja, mert rengeteg elégedetlen ügyfél jelentkezett volna, és ez ilyenkor a médiában is teret kap. Elképzelhető, hogy a Pénzügyi Felügyelet is elmarasztalta volna a bankot.

7.3.1.3. Az incidens utáni tevékenységek

Közvetlenül az incidens lezárása után elkészült a Post Mortem riport, amely túl azon, hogy tartalmazta a teljes kronológiát, értékelte is az incidenskezelés folyamatát, az incidensben érintett felhasználók és szakterületek felkészültségét, a reagálási időket, azt, hogy a belső és külső kommunikáció menynyire volt világos és érthető.

Ebben olvasható továbbá a Lessons Learned fejezet is, amelyben azon megállapítások szerepeltek, hogy mit lehetett tanulni az esetből, hol kell fejleszteni a folyamatokat, az incidenskezelési tervet.

Az incidens utáni hét folyamán a biztonsági terület folyamatos monitoringot végzett, hogy érkeztek-e újabb bejelentések, az interneten van-e visszhangja az adathalászatnak.

7.3.2. A vírusvédelmi incidens elhárítása

7.3.2.1. Az incidens előtti tevékenységek

A szervezet, akinek a neve legyen Berkenye Láng és Mémgyár Zrt. (továbbiakban BLM Zrt.) komoly IT biztonsági infrastruktúrát működtetett. Volt végpontvédelem a munkaállomásokon és laptopokon, volt vírusszűrés az Exchange szerveren, volt többféle víruskereső motorral ellátott web- és e-mail-tartalomszűrés. És volt oktatás, ahol a felhasználók részére bemutatták azon e-mail típusokat és jellemzőket,

amelyeket fel kellene ismerni mint potenciális veszélyforrások. Ráadásul az Információvédelmi Osztály (továbbiakban IVO), amennyiben értesült olyan esetről, hogy nagyobb mennyiségben érkezett kártevőt tartalmazó e-mail, arról figyelmeztetést tett közzé az intraneten.

7.3.2.2. Az incidens alatti tevékenységek

Az egyik hétköznap reggelen felhasználói bejelentés érkezett a kontrolling osztályról – akik jellemzően számlákkal dolgoznak –, miszerint érkezett egy Deutsche Telekom számlát tartalmazó elektronikus levél, és a felhasználó komolyan véve a benne szereplő figyelmeztetést, rákattintott a csatolt .pdf dokumentumra, ami után viszont látszólag nem történt semmi. Ekkor kezdett gyanús lenni a felhasználónak a dolog, és megtette a bejelentést telefonon az IVO-nak.

A szakértő kollégák – az incidenskezelési tervben szereplő intézkedéseket foganatosítva – megkérték a felhasználót, hogy a munkaállomásából húzza ki a hálózati kábelt, és ne nyúljon hozzá, amíg az IVO szakértő kollégája meg nem jelenik nála ellenőrizni, hogy történt-e fertőzés, illetőleg fut-e valamilyen kártevő a gépen. Egy másik szakértő közben az e-mail-szerverről legyűjtötte azon felhasználók listáját – összesen kilenc ilyen volt – akik megkapták ugyanezt a levelet. Egyesével végigtelefonálták a kollégákat, és helyzetjelentést kértek tőlük. A többség felismerte, hogy ez a levél gyanús, és kattintás nélkül törölte azt. Pár kolléga pedig még nem jutott el a levelezés feldolgozásában ehhez a küldeményhez, és volt, aki éppen szabadságát töltötte – az ő esetében az e-mail-rendszer adminisztrátora az IVO engedélyével törölte a postafiókból a levelet.

A szakértő kolléga közben odaért a hálózatról leválasztott munkaállomáshoz, és pendrive-ról több víruskereső programot lefuttatott a gépen. Éles fertőzést egyik sem talált. Magát a kártevőt hordozó levelet sem találta egyik vírusvédelmi program sem gyanúsnak, ebből arra lehetett következtetni, hogy olyan 0. napi sérülékenységet kihasználó kártevővel álltak a kollégák szemben, amelyet még nem azonosítottak a vírusvédelmi programokat gyártó cégek. A szakértő kolléga ezután a levelet annak csatolmányával együtt felmásolta a pendrive-jára, majd elküldte e-mailben azon vírusvédelmi cégek kutatási részlegeinek, akikkel a cég szerződésben állt, hogy azonosítsák a kártevőt, és adjanak ki hozzá friss adatbázist és eltávolító eszközt. Erre azért volt szükség, hogy a BLM Zrt. összes számítógépére leterítve a friss adatbázist, azokat is át lehessen vizsgálni.

Ezzel egyidőben az IVO-n a webtartalomszűrő naplóállományait elemezték a kollégák, és megállapították, hogy mivel a felhasználó olyan internethasználati jogosultsági csoportban volt, amelynek tagjai nem voltak jogosultak futtatható állományokat letölteni, így ezen a szűrőn megakadt a kártevő futtatható állománya. Miután megérkezett a vírusvédelmi cégtől a friss szignatúracsomag, azokat terítették az IT üzemeltető kollégák a munkaállomásokra, hogy a következő keresés már ez alapján fusson.

Azon kollégák esetében, akik kaptak a levélből, és azt mondták, törölték is azt, a biztonság kedvéért egy teljes víruskeresést indítottak.

Mivel nem történt tényleges fertőzés, az incidenskezelésbe nem kellett bevonni további területeket az IT üzemeltetésen kívül. Az incidenst lezárták..

7.3.2.3. Az incidens utáni tevékenységek

Az incidens után a belső intranetet kezelő PR szervezetet megkérték, jelentessen meg egy figyelmeztető hírt, amely arról szólt, hogy ismét felbukkantak az olyan levelek, amelyek valamilyen szolgáltató (Deutche Telekom, DHL, UPS) nevében küldenek valamilyen csatolmányt (számla, csomagértesítő stb.), illetve annak álcázott kártevőt. A megjelent hírben felszólították a felhasználókat, legyenek óvatosak, és amennyiben ilyennel találkoznak, ne kattintsanak rá, hanem töröljék, ha pedig rákattintottak, azonnal jelezzék az IVO-nak.

A Post Mortem riportot dokumentálták, amely túl azon, hogy tartalmazta a teljes incidenskezelési kronológiát, értékelte is az incidenskezelés folyamatát, az incidensben érintett felhasználók és szakterületek felkészültségét, a reagálási időket, azt, hogy a belső és külső kommunikáció mennyire volt világos és érthető. Ebben olvasható továbbá a Lessons Learned fejezet is, amelyben azon megállapítások szerepeltek, hogy mit lehetett tanulni az esetből, hol kell fejleszteni a folyamatokat, az incidenskezelési tervet.

Felhasznált irodalom

ISACA (Information Systems Audit and Control Association) (2012) COBIT 5. – Control Objectives for IT and Related Technology. Elérhető: https://cobitonline.isaca.org/ (a letöltés ideje: 2017. április 20.)

MSZT ISO/IEC 27001:2014. Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények

ISO/IEC 27002:2013 – Code of practice for information security management – essentially a detailed catalog of information security controls that might be managed through the ISMS

Informatikai biztonsági módszertani kézikönyv 8. sz. ajánlás (1994). Budapest, Miniszterelnöki Hivatal Informatikai Koordinációs Iroda Informatikai Tárcaközi Bizottság ajánlásai. Elérhető: www.uni-obuda.hu/users/horvath.zsolt.laszlo/_szakirodalom/ITB%20aj%C3%A1nl%C3%A1sok/ITB08.pdf (a letöltés ideje: 2017. április 20.)

Informatikai rendszerek biztonsági követelményei 12. sz. ajánlás (1996), Budapest, Miniszterelnöki Hivatal Informatikai Koordinációs Iroda Informatikai Tárcaközi Bizottság ajánlásai. Elérhető: https://dsd.sztaki.hu/mockups/itb/ajanlasok/a12/index.html (a letöltés ideje: 2017. április 20.)

Közigazgatási Informatikai Bizottság 25. számú ajánlása (2008). Budapest, Magyar Informatikai Biztonsági Ajánlások (MIBA) Elérhető: http://docplayer.hu/247021-Kozigazgatasi-informatikai-bizottsag-25-szamu-ajanlasa-magyar-informatikai-biztonsagi-ajanlasok-miba.html (a letöltés ideje: 2017. április 20.)

MUHA Lajos (2003): *Szabványok és ajánlások az informatikai biztonság területén*. VIII. Országos (centenáriumi) Neumann Kongresszus, előadás.

HUSMANN, Daniel (2004): *End Users: Assets or Liabilities When Handling a Cyber Incident?* SANS Institute. Elérhető: www.giac.org/paper/gsec/3783/users-assets-liabilities-handling-cyber-incident/106090 (a letöltés ideje: 2017. április 20.)

PARSONS, Kathryn – MCCORMAC, Agata – BUTAVICIUS, Marcus – FERGUSON, Lael (2010): *Human Factors and Information Security: Individual, Culture and Security Environment*. Command, Control, Communications and Intelligence Division DSTO Defence Science and Technology Organisation. Elérhető: www.dtic.mil/docs/citations/ADA535944 (a letöltés ideje: 2017. április 20.)

8. BIZTONSÁGI ESEMÉNYEK RENDÉSZETI SZEMPONTBÓL – A KIBERBŰNCSELEKMÉNYEK KEZELÉSE

Dr. Gyaraki Réka – Dr. Simon Béla

8.1. Biztonsági események rendészeti szempontból – a kiberbűncselekmények kezelése

8.1.1. Az informatikához kapcsolódó bűncselekmények és azok kezelése Magyarországon

Hétköznapi értelemben a bűnügyi rendőrség feladata, hogy nyomozás során elkapja a bűnözőket, összegyűjtse a bizonyítékokat, továbbítsák azokat az ügyészség felé, akik a vádat képviselik a bíróság előtt, ahol aztán elítélik, rácsok mögé juttatják az elkövetőket.

A helyzet azonban nem ilyen egyszerű, hiszen:

- nyomozásokat nemcsak a rendőrség, hanem a NAV bűnügyi szervei és az ügyészség is folytathat;
- az eljárásoknak csak egy része jut el a vádemelésig, ahol nem az összes vádlottat ítélik el, és akiket mégis, közülük sem kell feltétlenül mindenkinek ténylegesen letöltendő szabadságvesztés miatt büntetés-végrehajtási intézménybe vonulni;
- a nyomozó hatóságon és az ügyészségen kívül mások is részt vesznek az eljárásban;
- számos különleges eljárás is a büntetőeljárás részét képezi;
- a nyomozó hatóságoknak a terheltre nézve nemcsak a hátrányos, de a felelősségét csökkentő adatokat, tényeket is össze kell gyűjteniük;

A jogsértő cselekményeknek csak egy bizonyos része éri el azt a szintet, ami büntetőeljárás elrendelésének alapjául szolgálhat. A fennmaradó esetekből polgári peres vagy szabálysértési eljárás lehet.[1]

A büntetőeljárásról szóló törvény (1998. évi XIX. törvény, továbbiakban Be.) 608 paragrafusból áll. Mivel a jogrendszerünkben a vitás kérdések eldöntésének legsúlyosabb végkimenetelei ebből az eljárás típusból származhatnak, nagyon sok garanciális szabállyal ellátott és szerteágazó folyamat az, amit büntető eljárásnak hívunk.

Számos olyan bemenete van egy büntetőeljárásnak, amely nyomozás elrendelését teszi indokolttá. Ezek két csoportra oszthatók, melyek egyrészt a nyomozó hatóságok saját észlelései, másrészt lehetnek feljelentések, bejelentések.

Fontos megjegyezni, hogy a nyomozás elrendelését megelőzően lehetőség van titkos információgyűjtésre, illetve a feljelentés kiegészítésére is. Az előbbi lehetővé teszi a nyomozó hatóságok számára, hogy titkosszolgálati eszközök alkalmazásával gyűjtsenek bűnügyileg releváns információkat, bizonyítékokat,

[1] Egy becsületet sértőnek vélt kifejezés közlése nagy nyilvánosság előtt lehet bűncselekmény, nagy nyilvánosság nélkül már csak szabálysértés, de indokolatlanul bántó véleménynyilvánítás esetén lehet, hogy csak személyiségi jogok sérelme miatti polgári jogi kérdés.

míg az utóbbi speciális eljárás elrendelésére akkor kerül sor, ha a feljelentés alapján a nyomozás elrendeléséről, illetőleg a feljelentés elutasításáról megnyugtatóan nem lehet állást foglalni.[2]

De milyen okok vezethetnek arra, hogy büntető eljárás kerüljön elrendelésre? Alapvetően elég egy bűncselekmény elkövetésének a gyanúja. Annak eldöntése azonban, hogy egy adott cselekmény bűncselekmény-e, korántsem egyszerű. A 2012. évi C. törvényben kihirdetett Büntető Törvénykönyv (továbbiakban Btk.) szerint „bűncselekmény az a szándékosan vagy – ha e törvény a gondatlan elkövetést is büntetni rendeli – gondatlanságból elkövetett cselekmény, amely veszélyes a társadalomra, és amelyre e törvény büntetés kiszabását rendeli."[3] Nem egyszer előfordult már, hogy egy adott tényállással összefüggésben a nyomozó hatóság vádemelési javaslattal elküldte a nyomozás iratait az ügyészségre, akik az iratok alapján vádat emeltek, és végül a bíróság bűncselekmény vagy a cselekmény társadalomra vonatkozó veszélyességének hiánya miatt megszűntette az eljárást.

Ennek a sokszereplős, összetett „társasjátéknak" tehát bonyolult szabálykönyve van, melynek ismertetése meghaladja e tankönyv kereteit. Ugyanakkor alapvetésként kijelenthető, hogy minden olyan esetben, amikor józan ésszel azt feltételezzük, hogy súlyos jogsértés – vélhetően bűncselekmény – valósult meg, indokolt feljelentést tenni a bűncselekmény elkövetésének helye szerint illetékes rendőrkapitányságon.[4] Az már a nyomozó hatóság feladata, hogy eldöntse: történt-e bűncselekmény, és ha igen, azzal ki gyanúsítható.

Sok esetben nem indokolt konkrét személy ellen megtenni a feljelentést, mivel – különösen az informatika világában – könnyen elképzelhető, hogy egy adott cselekményt egy felhasználói fiókhoz vagy konkrét eszközhöz rendelt személyhez kötünk, holott később kiderül, hogy nem az általunk gyanúsított személy volt a tényleges elkövető. Ilyen esetben felmerülhet később hamis vád bűncselekményének elkövetése részünkről. Ennek elkerülése érdekében indokolt a feljelentést ismeretlen tettessel szemben megtenni, még akkor is, ha szinte teljesen biztosak vagyunk az általunk gyanúsított személy bűnösségében, és még akkor is, ha a feljelentés kifejtésében konkrétan nevesítjük azt a személyt, aki a feljelentett cselekményhez köthető.[5]

A bűncselekmények nyomozását a büntetőeljárásról 1998. évi XIX. törvény rendelkezései alapján a nyomozó hatóság az ügyész rendelkezése alapján vagy önállóan végzi. A rendőrség általános nyomozó hatóság.

A törvény rendelkezése alapján – különös illetékességgel – a Nemzeti Adó- és Vámhivatal végzi egyes bűncselekmények miatt a nyomozást, továbbá külföldön lévő magyar kereskedelmi hajón vagy polgári légi járművön magyar állampolgár vagy – meghatározott esetben – bárki által elkövetett bűncselekmény miatt a hajó, illetve a légi jármű parancsnoka jogosult a nyomozó hatóságra vonatkozó rendelkezések alkalmazására. Ugyancsak különös illetékesség alapján a nyomozó hatóságok, a legfőbb ügyész engedélyével, a külön törvényben meghatározott feltételek esetén az Európai Unió tagállamainak nyomozó hatóságai, továbbá az Európai Rendőrségi Hivatal (EUROPOL) részvételével egy ügyre vagy ügyek meghatározott csoportjaira közös nyomozó csoportot alakíthatnak, illetőleg abban részt vehetnek.

A klasszikus bűncselekmények mellett néhány évtizede jelentek meg azok a tilalmazott magatartások, amelyeket valamely jellemvonásuk, így leggyakrabban az elkövetés eszköze (informatikai-, számítógépes-, számítástechnikai, internet stb.) alapján nevezhetünk el. A számítógéppel kapcsolatos deliktumok egy részére jellemző, hogy a támadás céljai maguk a számítógépek, a kommunikációs berendezések,

---

[2] A feljelentés kiegészítése során a feljelentés kiegészítést végző hatóság a 178. § (1) bekezdésében meghatározott egyéb adatszerző tevékenységet folytathat, a feljelentőt meghallgathatja, stb. Ennek határideje maximum 30 nap.

[3] Elérhető: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200100.TV (a letöltés ideje: 2017. április 20.)

[4] Annak eldöntése azonban szintén nem egyszerű kérdés, hogy mi az elkövetés helye. Valaki vonaton utazik Budapestről Bécsbe, és valahol útközben megtekint egy Miskolcon feladott hirdetést egy szegedi szerveren üzemeltetett apróhirdetés oldalon, aztán elutalja a pénzt a csalónak az országhatár túloldalán, aki azt egy paksi ATM-ből felveszi. Nem egyszerű, de a hatóságok dolga eldönteni, hogy kit érjen a nyomozási feladatok ellátásának dicső lehetősége. A valóságban a nyomozó hatóságok inkább annak lehetőségét keresik, miként tudják egy másik nyomozó hatóság hatáskörét, illetékességét megállapítani azért, hogy a feladat alól mentesüljenek. (A példában egyébként a „tévedésbe ejtődés" adja az elkövetés helyét, azaz ahol a sértettben a téves képzet kialakult, ami alapján utalt.)

[5] Kisarkítva: „Feljelentést teszek ismeretlen tettes ellen az alábbiak miatt: a frissen kirúgott Gipsz Jakab bement a szerverterembe, és amikor fél órával később kijött számos szerver merevlemeze le volt formázva." – ebben az esetben is tudni fogja a nyomozóhatóság, hogy minden bizonnyal Gipsz Jakab az elkövető, de a hamis vád fel sem merül – például, ha furcsa módon ebben az időben más okból törlődtek az adatok.

adatátviteli hálózatok és az abban fellelhető adatok. Az elkövetői szándék azonban irányulhat ezen eszközök felhasználásával más, hagyományos értékekre is.

Az információs társadalom új típusú bűncselekményeinek alapvető jellemzője tehát, hogy az információ mint vagyoni értéket megtestesítő dolog és annak környezete válik a bűncselekmények tárgyává. Az információvédelemnek az információk tulajdonosainak és/vagy hordozóinak a gazdasági érdekeit kell figyelembe vennie, valamint azokét is, akiket az információk tartalma érint. Utóbbihoz megemlítendők a privacy, azaz a személyiségi jog védelmével kapcsolatos követelmények, elsősorban az elektronikus adatfeldolgozás miatt. Tehát a társadalomban megjelent elektronikus információs rendszer nemcsak a vagyoni érték vagy a gazdasági érdek oldaláról jelent védendő értéket, hanem a közérdek vagy a magánérdek megtestesítőjeként is. Mindezeket a szempontokat az egyes büntetőjogi tényállásban kell megjeleníteni, olyan terminológiák megfogalmazásával, amelyek eleget tesznek az informatikai elvárásoknak, a jogalkotási követelményeknek, továbbá a jövőbeni technológiai fejlődés kihívásainak.

Az *informatikai bűncselekmény* fogalmára egyetlen definiciót sem rögzítettek. Ugyanakkor találkozhatunk a *számítástechnikai bűncselekmény* és az *internetes bűncselekmény* megkülönböztetésével.[6]

Ahogy már utaltunk rá, a fogalom tartalmában több tudomány szakterületét érintik, de egyben nemzetközi vonatkozásai is vannak. A nemzetközi gyakorlat a *számítógépes bűncselekmények* meghatározása során – a számítástechnikai rendszerre és az adatra mint elkövetési tárgyakra figyelemmel – az *adat* fogalmának tisztázására törekszik. A Cyber-crime Egyezmény[7] és az EU kerethatározat[8] megfogalmazása szerint a *számítástechnikai adat* tényeknek, információknak, illetőleg fogalmaknak minden olyan formában való megjelenése, mely számítástechnikai feldolgozásra alkalmas, ideértve azon programot is, mely valamely funkciónak a számítástechnikai rendszer által való végrehajtását biztosítja.[9] Tehát az adatnak, beleértve a feldolgozásához szükséges programot, számítástechnikai feldolgozásra alkalmasnak kell lennie.

Ez az „alkalmassági feltétel" vezet el, amennyiben a számítástechnikai rendszert és az adatot mint elkövetési tárgyat tekintjük, az *információ*- illetve az *adatbiztonság* fogalomrendszeréhez. Az információs és informatikai rendszerekben olyan előírások betartását kell követelménynek tekinteni, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik. Mindebből következően tehát a számítástechnikai adatot az előbbiekben körülírt minőségében büntetőjogi védelemben kell részesíteni.

A nemzeti szabályozás a számítástechnikai rendszer és adatok elleni bűncselekmények (tiltott adatszerzés, információs rendszer vagy adat megsértése, információs rendszer védelmét biztosító technikai rendszer kijátszása tényállásokat) a 2012. évi C. törvényben[10] történt meg.

8.1.2. A kiberbűncselekmények jellemzői

A nyomozó hatóság munkáját a következő pontokban összeszedett tényezők nehezítik:

A számítástechnikai bűncselekmények végeredménye, leginkább az azt elszenvedők számára, olyan gyorsasággal következik be, hogy azt nem is észlelik az adott pillanatban. A *gyorsaság* tehát nem azt jelenti, hogy az elkövetők egy adott helyzetet kihasználva gyorsan követik el a deliktumot, ahogy például a lopás esetében, hiszen a bűncselekmény előkészülete – például egy számítástechnikai program megírása – több órát vagy napokat vehet igénybe, hanem az eredmény (az adatokhoz való hozzáférés, módosítás, megváltoztatás stb.) az, ami gyorsan történik meg. Éppen ezért könnyű a bűnelkövetők helyzete,

---

[6] Infokommunikációsjog.hu szerint Számítástechnikai bűncselekmények azok a deliktumok, melyek egy számítástechnikai rendszerrel vagy számítástechnikai adattal kapcsolatba hozhatóak, akár úgy, hogy az elkövetés eszközeként jelennek meg vagy pedig a bűncselekmény tárgyát képezik. Az internetes bűncselekmények pedig információs rendszerek ellen vagy felhasználása által elkövetett bűncselekmények.

[7] Az Európa Tanács 2001. november 23-án Budapesten fogadta el a Számítástechnikai bűnözésről szóló egyezményt (Cybercrime)

[8] A Tanács 2005/222/IB kerethatározata az információs rendszerek elleni támadásokról (2005); valamint Az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról

[9] Cybercrime 1.Cikk. b) pont)

[10] 2012.évi C. törvény a Büntető Törvénykönyvről XLIII. Fejezet Tiltott adatszerzés és az információs rendszer elleni bűncselekmények

és nehéz a nyomozó hatóságok feladata. A gyorsaság nemcsak az adatok, információk sebességét jelenti, hanem a technika fejlődését is, mellyel lépést kell tartani. A (potenciális) sértettek fokozott veszélyben vannak, hiszen előfordulhat, hogy nem észlelik időben a sérelmükre elkövetett bűncselekményt, vagy annyi idő telik el az elkövetés óta, ami már a nyomozást is megnehezíti. A gyorsaság függ a kor technikai újításaitól és az elkövetők szakmai fejlettségétől, tudásától.

A számítástechnikai bűncselekmények esetében a gyors elkövetés mellett, illetve azzal párhuzamosan a *látencia* az, amely miatt elmondható, hogy a számítógépes bűncselekmények áldozatai egyáltalán nem vagy nem időben észlelik, hogy bűncselekmény áldozatai lettek. A sértettek, mivel a jogsértés a virtuális térben történik, nem veszik észre, hogy az informatikai rendszerben tárolt adataikkal visszaéltek. A látencia esetében szükséges kiemelni azt is, hogy – akár a magánszektorban, akár az állami szektorban következett be a támadás (például DDOS támadás vagy Ransomware esetében) –, sokszor egyszerűen eltitkolják a tényt, hogy az adatokhoz, esetleg a számlákhoz illetéktelenek hozzáfértek. Főleg bankok vagy nagyobb cégeknél a bűncselekményeket és/vagy az esetek többségét nem jelentik a hatóságok felé.[11] Sok esetben azért, mert attól félnek, hogy az ügyfeleik bizalma meginog. Másik oka a magas fokú látenciának, hogy az elkövetőknek nem szükséges az elkövetés helyszínén tartózkodni. A különböző kommunikációs eszközök segítik, hogy a cselekményüket távolról irányíthassák, így a tettenérés szinte kizárt, a nyomozó hatóság részéről a felderítés a hagyományos eszközökkel lehetetlen. Nehezíti a nyomozói munkát az is, hogy a bűnözők nemcsak, hogy távolról irányítják az eszközöket, hanem előfordulhat az is, hogy időzítik az adott programot, amely így meghatározott időben hajtja végre a módosításokat, szerzi meg az adatokat az áldozatok eszközeiről.

A kibertérben a elkövetőket fizikai korlátok sem tartják vissza a jogellenes cselekményüktől. Az internet nem ismeri az országhatárokat, a számítógépes bűnözés – ahogy az ismert nigériai csalások esetében is – nemzetközi jelleggel bír. Az információ áramlását nem nehezíti meg, hogy azt esetlegesen az óceánon túlra kell eljuttatni, hiszen minden a virtuális térben történik, így az elkövetők helyzetét sem rontja, ha fizikailag nincsenek egy helyen az áldozataikkal. Interneten a névtelenség álarca mögé bújhat bárki. Ezekből a jellemzőkből is egyértelműen látszik, hogy ez a tér ideális az elkövetők számára. Szintén kedvez, hogy az internet hatalmas adatállományát, az adatforgalmat nem lehet ellenőrizni, így a visszaéléseket nagyon nehéz nyomon követni.

A számítógépes bűnözés rendkívüli mértékben függ *a technológia, technika szintjétől.* A bűnözők minden újabb és újabb számítástechnikai terméket fel tudnak használni a bűncselekmények elkövetése során. Amint kifejlesztenek egy újabb számítástechnikai vívmányt – nem feltétlen csak hardverekre kell gondolni, de szoftverekre is – a bűnözők idővel felhasználjak azokat az elkövetés során. A legnagyobb problémát az jelenti, hogy sem a hatóságok, sem a társadalom nincsenek felkészítve e bűnözés elleni védelemre, és elmondható, hogy az elkövetőkkel szembeni hatósági fellépés bizonyos országokban – elsősorban anyagi okok miatt – nem megfelelő, sőt már az e bűnözéssel szembeni védekezés sem megfelelő szintű.

A számítógépes bűncselekmények elkövetését nehezen vagy csak későn lehet észlelni, s ezt a folyamatot a nyomozó hatóságok járatlansága, képzetlensége, esetlegesen technikai elmaradottsága értelemszerűen nem gyorsítja. A felhasználók névtelensége vagy álnevek használata miatt nehéz a személyazonosság beazonosítása, továbbá az adatok titkosítása, megsemmisítése is ellehetetleníti a felderítést. Mindemellett pedig az informatikai eszközök és berendezések helyrehozhatatlan megrongálása is megnehezíti a nyomozó hatóság munkáját.

A számítógépes bűnözés többnyire *intellektuálisnak* nevezett bűnözési forma. Az elkövetők általában fiatal, magasan képzett, magas intelligenciájú (szak)emberek. Az intellektuális jelleg nem minden informatikai deliktum esetén igaz, hiszen vannak olyan bűncselekmény-típusok, melyek nem igényelnek nagy szakképzettséget, mégis jelentős károkat képesek okozni. A bűncselekményeket sokszor jómódú, többrétűen szocializálódott, 18 és 45 év közötti emberek (jellemzően férfiak) követik el.

[11] Sok esetben a pénzintézetek, hitelintézetek nem jelentik, hogy akár ők maguk, vagy az ügyfeleik támadás áldozatai lettek.

Ahogy korábban már volt róla szó, a világháló névtelenséget biztosít. Jelenleg nincs olyan hazai vagy nemzetközi jogszabály, amely büntetné azokat, akik egyáltalán nem adják meg nevüket, adataikat, vagy fiktív névvel regisztrálnak. Ez az, ami miatt a számítógépen elkövetett bűncselekmények száma felfelé ível.

8.1.3. A számítógépes bűncselekmények elkövetési területei

A számítástechnikai bűncselekmények elkövetése jellemzően anyagi, gazdasági és pénzügyi haszonszerzési célzattal történik. Az informatikai rendszerekben adatok formájában tárolt információk védelmet igényelnek, erre az *információvédelem* vonatkozik. Ez olyan eljárások és intézkedések összességét jelenti, amely lehetővé teszi az azonosítási és hitelesítési eljárások kialakítását, a hozzáférési rendszer létrehozását (a jogosultságok kiosztását, ellenőrzését), az adatok és a programok sérthetetlenségének biztosítását, az adatok bizalmasságának garantálását (titkosság: az információkhoz vagy adatokhoz csak az arra jogosultak, és csak az előírt módon férhetnek hozzá), a naplózási rendszer megvalósítását a szervezeten belül. A különböző védett, bizalmas adatok sértetlenségéhez fűződő érdek kiemelten fontos; illetéktelen személyek vagy csoportok általi megszerzésük nemcsak komoly károkat okoz, de az elkövetőknek jelentős bevételi forrást is jelenthetnek. A rendvédelem, igazságügy vagy nemzetbiztonság területén ez *a személyes, illetve minősített adatok illetéktelen megszerzése.*

Az informatikai bűncselekmények kezelésével kapcsolatos nyomozást végző szervezetek között – a felderítés sikerességének biztosítékaként – szükséges a mind az érintett országon belüli, mind az annak határain átnyúló, nemzetközi együttműködés. Ennek hatékonysága érdekében a rendőrség tagja több nemzetközi igazságügyi szervezetnek, s ez megkönnyíti az információáramlást és -cserét, ezzel is elősegítve a kiberbűnözés mint szervezett bűnözési forma visszaszorítására tett lépéseket. Az országhatárokon átnyúló együttműködéssel kapcsolatos szabályozást mind a hazai jogi, mind pedig a nemzetközi együttműködésekre vonatkozó szerződések, irányelvek tartalmazzák.

Magyarországon az egyik legkiemelkedőbb szervezete a rendőrségnek a Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztálya, amely jelenleg három osztályra tagolódva lát el nyomozati feladatokat. Az egyik osztály magát a nyomozati munkát, a másik a forenzikus feladatokat, míg a harmadik osztály a felderítést, vagyis a bírói engedélyhez kötött titkos adatszerzést folytatja le.

A rendőrség másik kiemelkedő szerve a Budapesti Rendőr-főkapitányság Korrupciós és Gazdasági Bűnözés Elleni Főosztály Pénzhamisítás és Csúcstechnológiai Bűnözés Elleni Alosztály, amely a hagyományos nyomozati feladatok mellett szintén szakirányítási feladatokat lát el a budapesti kerületi kapitányságok felé.

A 25/2013. (VI. 24) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről az egyes bűncselekmények tekintetében a Reptéri Rendőrségi Igazgatóságot is jogokkal ruházta fel a számítástechnikai környezetben elkövetett bűncselekmények egyes tényállásainak nyomozásával kapcsolatban.

Az elmúlt időszakban a leggyakrabban elkövetett kibertámadások, illetve -bűncselekmények a DDoS támadások, illetve a Ransomware-ek vagy zsarolóvírusok által kivitelezettek. Ez a két támadási forma érheti az otthoni felhasználót, de érintette vállalkozások, illetve állami és önkormányzatok információs rendszerét is.

Az információs rendszerek elleni támadások célja lehet többek között a zsarolás, a pénzszerzés, politikai vagy ideológiai célok. Ezek felderítésénél, kezelésénél már nem egy hagyományos rendőri szemlélet szükséges, a nyomozásnak sokkal több mindenre ki kell terjednie.

Először is a Btk.-ban rögzített minősítését fontos felidézni. A 2012. évi C. törvény 423. §-a rendelkezik az információs rendszer vagy adat megsértésének ügyéről. Az információs rendszer vagy adat megsértésének tényállásába ütköző bűncselekmény elkövetése esetén mindig az illetékességgel rendelkező rendőrkapitányság felé feljelentéssel – akár személyesen szóban vagy írott formában – kell élni. A GovCert ilyen esetben nem javasolja, hogy a sértett engedjen a zsarolásnak, és megfizesse a váltságdíjat. A bűncselekmény elkövetése esetén mindig vizsgálni kell az elkövetés helyét, amely a kiberdeliktumok

esetén speciális. Mivel a kibertér nem egy behatárolt helyszín, terület, így mindig az a nyomozó hatóság köteles eljárni, akinek az illetékességi területén először tettek feljelentést.

A feljelentés esetén a hatóságnak 3 nap áll rendelkezésre, hogy az abban foglaltakat megvizsgálja, és az alapján elrendelje a nyomozást, vagy elutasítsa, illetve a feljelentés kiegészítését írja elő.

A nyomozó hatóság tudomására kell hozni minden olyan tényt vagy információt, amely alapján a nyomozást le lehet folytatni.

Amennyiben a rendőrség a rendelkezésre álló adatok alapján elrendeli a nyomozást, úgy a feljelentésben foglaltakat egy, de akár több alkalommal is kihallgatás formájában tisztázhatja, pontosíthatja. Ennek során érdemes valamennyi információt maradéktalanul a rendelkezésre bocsátani.

A rendelkezésre bocsátott információk mellett a rendőrségnek lehetősége van az 1998. évi XIX. törvény, a büntetőeljárásról szóló törvény 71. §-a alapján megkereséssel élni a szolgáltató(k) felé, akik a megkeresésben foglaltaknak megfelelően kötelesek eljárni, akár ügyészi engedéllyel vagy anélkül.

Az egyik legfontosabb kiindulópont lehet az IP-cím beazonosítása. Ilyennel valamennyi világhálóra feljelentkezett számítástechnikai eszköz rendelkezik, ugyanakkor – amennyiben az elkövetők nyilvános számítógépet használtak, vagy technikai úton meg tudták változtatni az IP-címüket – a sikeres beazonosítás nem minden esetben vezet el az elkövetőhöz.

8.1.4. Az információcserére vonatkozó hazai és nemzetközi jogi szabályozások

A 2009/315 IB kerethatározata alapján egy tagállam központi hatósága megkeresést küldhet egy másik tagállam központi hatósága részére bűnügyi nyilvántartásban szereplő információk kiadásáért, büntetőeljárás céljából vagy büntetőeljárástól eltérő célból.

Ezek az anyagok magukban foglalhatnak:

- az érintett személy állampolgársága szerinti tagállamban hozott és a bűnügyi nyilvántartásba bejegyzett ítéleteket;
- a más tagállamban hozott, azonban általa őrzött ítéleteket;
- a más tagállamokban hozott és a bűnügyi nyilvántartásba bejegyzett ítéleteket;
- harmadik országban hozott, majd később a tagország számára továbbított, a bűnügyi nyilvántartásba bejegyzett ítéleteket.

Ha egy személy a bűnügyi nyilvántartásban a rá vonatkozó információ közlésére irányuló kérelmet nyújt be, úgy az adott tagállam megkeresheti egy másik tagállam központi hatóságát bűnügyi nyilvántartásban szereplő információk kiadásért.

A határidő tekintetében főszabály, hogy haladéktalanul, de legkésőbb a kérelem kézhezvételének időpontjától számított 10 munkanapon, ha a megkeresés egy adott személytől származik, úgy 20 munkanapon belül, teljesíteni kell a megkeresést.

Bűnügyi nyilvántartások, illetve az azzal kapcsolatos tájékoztatás: az *Európai Kölcsönös Jogsegélyegyezmény.* Ennek rendelkezései alapján:

- a részes államok kötelezettséget vállalnak arra, hogy egy adott büntetőügyben való felhasználás érdekében, a bűnügyi nyilvántartásukban rendszerezett adatokról kivonatot készítenek, illetve felvilágosítást adnak egy másik részes állam igazságügyi hatóságának a megkeresése alapján, feltéve, hogy ezt saját igazságügyi hatóságai részére is megtennék. Ezt meghaladóan a megkereséseket a megkeresett állam saját szabályai és gyakorlata alapján teljesítik;
- az igazságügyi minisztériumok évente minimum egy ízben tájékoztatást nyújtanak egymás részére azokra a büntetőítéletekre, valamint az azt követő intézkedésekre vonatkozóan, amelyeket más részes államok állampolgáraival szemben hoztak és alkalmaztak, és amit bűnügyi nyilvántartásukba is bejegyeztek. Amennyiben az érintett személy több részes állam állampolgára is, úgy a tájékoztatás valamennyi államra kiterjed. Kivételt képez ez alól, ha az érintett személy annak a részes államnak az állampolgára, amelynek a területén elítélték.

A megkeresés teljesítésére vonatkozó kötelezettség csak akkor érvényes, ha a nyomozás a következőkre irányul:

– a megkereső államban legkevesebb négy, a megkeresett államban legkevesebb két év szabadságvesztéssel vagy szabadságelvonással járó intézkedéssel sújtandó bűncselekményre;
– az 1995. évi, az Európai Rendőrségi Hivatal létrehozásáról szóló egyezmény (Europol-egyezmény) 2. cikkében, illetve e módosított egyezmény mellékletében említett bűncselekményre;
– amennyiben az Europol-egyezmény nem rendelkezik róla, az 1995. évi, az Európai Közösségek pénzügyi érdekeinek védelméről szóló egyezményben, vagy annak az 1996. évi jegyzőkönyvében vagy az 1997. évi második jegyzőkönyvében említett bűncselekményre.

A Nemzeti Adó-és Vámhivatal hatáskörébe tartozik:

- a bitorlás (Btk. 384. §);
- a szerzői vagy szerzői joghoz kapcsolódó jogok megsértése (Btk. 385. §);
- a védelmet biztosító műszaki intézkedés kijátszása (Btk. 386. §);
- jogkezelési adat meghamisítása (Btk. 387. §);
- iparjogvédelmi jogok megsértése (Btk. 388. §).

A NAV Központi Nyomozó Főosztály Információ-Technológiai Osztálya a 2016-os évben a szerzői vagy szerzői jogokhoz kapcsolódó jogok bűncselekményével kapcsolatban több, mint 2,2 milliárd forintnyi elkövetési érték miatt folytattak le eljárást.[12]

8.1.5. A kiberbűncselekményekhez kapcsolható egyéb szervezetek

Az informatikával kapcsolatos jogsértések sokszor összeköthetők a kibervédelem és a kiberbiztonság körével is. Bizonyos esetekben nemcsak a már említett nyomozó hatóságok végzik az informatikához kapcsolódó bűncselekmények kezelését, hanem – például DoS vagy DDoS támadások esetében, amelyek akár kormányzati weboldalakat vagy kritikus infrastruktúrákat érinthetnek – ez a feladat már szorosan kapcsolódhat a nemzetbiztonsági feladatokat ellátó szervezetekhez, valamint egyéb hatóságok munkájához is, amelyek nem nyomozást végző, és nem nemzetbiztonsággal foglalkozó egységek.

8.1.5.1. A Nemzetbiztonsági Szakszolgálat

A Nemzetbiztonsági Szakszolgálat (NBSZ) feladata eltér a többi nemzetbiztonsági szervezet munkájától; a kiberbűncselekményekkel és a kibervédelemmel kapcsolatos feladatokat is ellát, ugyanakkor a nyomozó hatóság munkájában is – felkérés alapján – részt vesz.

Feladata, hogy Magyarország nemzetbiztonsági védelmét ellássa úgy, hogy a bűncselekmények megelőzését és felderítését, valamint az igazságszolgáltatás hatékonyságát segíti elő. Magasan képzett szakembereivel, folyamatosan fejlesztett eszközeinek és módszereinek alkalmazásával nyújt titkos információgyűjtési és adatszerzési, továbbá szakértői szolgáltatásokat az igénybevételre törvényi jogosultsággal rendelkező nemzetbiztonsági és bűnüldöző szerveknek. Az NBSZ a rá vonatkozó törvények – többek között Magyarország Alaptörvénye, az 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról, valamint további törvények és kormányrendeletek – betartásával a jogszerűség, a szakszerűség és az átláthatóság biztosításával védi a jogállami követelmények teljesülését, és folyamatosan erősíti a Szakszolgálat és a nemzetbiztonsági tevékenység iránti közbizalmat.

[12] www.nav.gov.hu/nav/bunugy/eredmenyeink/bunugyi_szakterulet_eredmenyei_2016.html (letöltve: 2017. március 7.)

8.1.5.2.A Nemzeti Kibervédelmi Intézet

A Nemzetbiztonsági Szakszolgálat (NBSZ) egyik szervezete a Nemzeti Kibervédelmi Intézet (NKI), amelyben három szervezeti egység különül el a tevékenységüknek megfelelően: a Nemzeti Elektronikus Információbiztonsági Hatóság, a Kormányzati Eseménykezelő Központ incidenskezelési szakterülete, valamint a Biztonságirányítási és Sérülékenységvizsgálati terület.

A Nemzeti Kibervédelmi Intézet feladata többek között az incidenskezelés, amelyet a 24 órás ügyeleti szolgálattal, valamint koordinációs és technikai támogatás biztosításával látnak el. Az NKI feladata továbbá a tudatosítás: kibervédelmi gyakorlatok koordinálása és végrehajtása.

Az egyik legfontosabb feladata a nemzetközi és az országon belüli együttműködés (többek között a rendvédelmi és a nemzetbiztonsági szervekkel).

A Nemzeti Kiberbiztonsági Intézet egyik szerezeti egysége a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH), amelynek feladata az ügyfelek és rendszerek nyilvántartása, a biztonsági osztályba és szintbe sorolásnak, illetve a követelmények teljesülésének ellenőrzése, valamint a sérülékenységvizsgálat elrendelése. Ez a szerv tesz javaslatot a létfontosságú rendszerek kijelölésére, valamint az információbiztonsági felügyelő kirendelésére.

A NEIH elbírálja az Ibtv. hatálya alá tartozó elektronikus információs rendszerek biztonsági osztályba sorolását és ellenőrzi az erre, valamint a szervezetek biztonsági szintbe sorolására vonatkozó jogszabályi követelmények teljesülését is.

Mindezek mellett a rendelkezésre álló információk alapján kockázatelemzést végez.

Éves ellenőrzési terv alapján az érintett ügyfeleknél ellenőrzi az információbiztonsági követelményeknek való megfelelést. Elrendeli az ellenőrzése során feltárt vagy máshogy tudomására jutott biztonsági rések elhárítását. Éves jelentést készít a Kormány számára az elektronikus információs rendszerek biztonságával, a létfontosságú információs rendszerelemek védelmével és a kibervédelem helyzetével kapcsolatban. További feladatai az Elektronikus Ügyintézési Felügyelettel történő együttműködés az elektronikus ügyintézési szolgáltatókra vonatkozó biztonsági követelmények biztosításában, valamint együttműködik a Kormányzati Eseménykezelő Központtal, valamint a Nemzeti Kiberbiztonsági Koordinációs Tanáccsal is. Ellenőrzi az információbiztonsági követelmények megtartását a különböző forrásokból megvalósuló fejlesztési projektek tervezési szakaszában, és részt vesz a Nemzeti Kiberbiztonsági Koordinációs Tanács által felügyelt információtechnológiai, hálózatbiztonsági, információmegosztási és incidenskezelési munkacsoportokban.

A NEIH javaslatot tehet létfontosságú információs rendszerelemek kijelölésére, információbiztonsági, létfontosságú információs infrastruktúravédelmi, kibervédelmi gyakorlatokat szervezhet. Véleményezheti a Kormányzati Eseménykezelő Központnak a biztonsági eseményekre való reagálás ágazatközi szabályairól és felelősségi köreiről szóló tervezetét. Indokolt esetben eljárási bírságot szabhat ki nem költségvetési szervekre; költségvetési szervekhez információbiztonsági felügyelő kirendelését javasolhatja. Az ügyfelek biztonságtudatosságának fejlesztésére oktatási anyagokat dolgozhat ki, felvilágosító kampányokat szervezhet. Felkérésre képviselheti Magyarországot a nemzetközi információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokon.

A Kibervédelmi Intézet másik szervezeti egysége a *Kormányzati Eseménykezelő Központ,* amely az incidenskezeléssel kapcsolatos területekért felelős. Feladatai közé tartozik a biztonsági események kezelése, a fenyegetésmenedzsment, az ügyeleti szolgálat biztosítása, az elemzés és az értékelés. Kibervédelmi gyakorlatokat dolgoz ki és tart, ennek révén feladata az általános képzés és tudatosítás. A Kormányzati Eseménykezelő Központ végzi a biztonságirányítás és a sérülékenység vizsgálatát, s támogatja a felelősök kijelölését. Biztonsági esemény kivizsgálása során együttműködik az internetszolgáltatókkal. Rendszeres vezetői tájékoztatást ad, s ellátja az EMIR/FAIR rendszerekkel kapcsolatos informatikai biztonsági feladatokat.

A Nemzeti Kibervédelmi Intézet szakmai kapcsolatot ápol számos CERT-tel és nemzetközi kibervédelmi szervezettel, úgymint:

- European Network and Information Security Agency – ENISA;

- Forum of Incident Response and Security Teams – FIRST;
- Trusted Introducer – TI;
- International Watch and Warning Network – IWWN;
- Central European Cyber Security Platform (Visegrádi Négyek és Ausztria kiberbiztonsági szervezeteit tömörítő platform).

A nemzetbiztonsági szervek, melyeket a már említett 1995. évi CXXV. törvény a nemzetbiztonsági szervezetekről (Nbtv.) sorol fel, két alkategóriába sorolhatók. Az egyik a polgári nemzetbiztonsági szolgálatok kategóriája. Ebbe tartozik az Alkotmányvédelmi Hivatal, az Információs Hivatal, a Terrorelhárítási Információs és Bűnügyi Elemző Központ és a Nemzetbiztonsági Szakszolgálat.

A másik alkategória a Katonai Nemzetbiztonsági Szolgálaté.

A nemzetbiztonsági szolgálatok a munkájukat külön törvényben szabályozott keretek között végzik, titkos információgyűjtéssel. A nemzetbiztonsági szervezetek közül elsősorban az Alkotmányvédelmi Hivatalt (röviden AH) kell megemlíteni, amelynek feladatát az Nbtv. határozza meg.

8.1.5.3. Az Alkotmányvédelmi Hivatal

Az Alkotmányvédelmi Hivatal (AH) feladatai többek között a felderítés és az elhárítás. Mindez az informatikához kapcsolódó bűncselekmények kezelése kapcsán valósul meg. Az AH felderíti és elhárítja:

- a magyar vagy akár külföldi titkosszolgálatok hazánk ellen irányuló törekvéseit;
- a Magyarország törvényes rendjének törvénytelen eszközökkel történő megváltoztatására vagy megzavarására irányuló leplezett törekvéseket;[13]
- a Magyarország gazdasági, tudományos-technikai, pénzügyi biztonságát veszélyeztető leplezett törekvéseket, valamint a jogellenes kábítószerés fegyverkereskedelmet;[14]
- ellátja a központi államhatalmi és kormányzati tevékenység szempontjából fontos szervek (intézmények) és létesítmények biztonsági védelmét.[15] Ez alatt érthetjük többek között a kritikus infrastruktúráknak minősülő létesítmények fizikai és információs rendszereik ellen irányuló támadásokkal kapcsolatos védelmét;
- közreműködik a nemzetközileg ellenőrzött termékek és technológiák jogellenes forgalmának felderítésében, megelőzésében, megakadályozásában és legális forgalmának ellenőrzésében.[16]

8.1.5.4. Az Információs Hivatal

Az Információs Hivatal (IH) feladata a kiberbiztonság területén többek között az, hogy megszerezze, elemezze, értékelje és továbbítsa a kormányzati döntésekhez szükséges, a külföldre vonatkozó, illetőleg külföldi eredetű, a nemzet biztonsága érdekében hasznosítható információkat. Továbbá Magyarország érdekeinek érvényesítését szolgáló tevékenységet folytat:

- felderíti a Magyarország függetlenségét, politikai, gazdasági vagy más fontos érdekét sértő vagy veszélyeztető külföldi titkosszolgálati törekvéseket és tevékenységet;
- információkat gyűjt a nemzetbiztonságot veszélyeztető, külföldi szervezett bűnözésről, különösen a terrorszervezetekről, a jogellenes kábítószerés fegyverkereskedelemről, a tömegpusztító fegyverek és alkotóelemeik, illetve az előállításukhoz szükséges anyagok és eszközök jogellenes nemzetközi forgalmáról;

[13] 1995. évi CXXV. tv. 5. § b) pontja
[14] 1995. évi CXXV. tv. 5. §. d) pontja
[15] 1995. évi CXXV. tv, 5. § e.) pontja
[16] 1995. évi CXXV. tv. 5. § k.) pontja

– felderíti az ország gazdasága biztonságának és pénzügyi helyzetének veszélyeztetésére irányuló külföldi szándékokat és cselekményeket;
– közreműködik a nemzetközileg ellenőrzött termékek és technológiák jogellenes forgalmának felderítésében és megelőzésében;
– ellátja a kormányzati tevékenység szempontjából fontos, külföldön lévő magyar szervek (intézmények) és létesítmények biztonsági védelmét;
– ellátja a hatáskörébe tartozó személyek nemzetbiztonsági védelmének, valamint objektumai műveleti védelmének feladatait, illetve elvégzi személyi állománya, valamint a hatáskörébe tartozó más személyek nemzetbiztonsági ellenőrzésének feladatait;
– végzi a minősített adatok védelmére használt rejtjelző eljárások, algoritmusok, valamint az országhatáron kívül rejtjelzésre használt eszközök kriptográfiai bevizsgálását és minősítését, továbbá rejtjelkulcsot állít elő.

8.1.5.5. A Katonai Nemzetbiztonsági Szakszolgálat

Jelen tanulmány az információs társadalom egyes elemei közül a honvédelmi ágazatot érintő szabályozást tekinti át. A honvédelmi célú elektronikus információs rendszerre vonatkozó szabályok legalább hét jogszabályban (törvény és kormányrendelet) fogalmazódtak meg, és módosították is ezeket. Az ágazati jogalkalmazók feladata tehát nem egyszerű, nem is csak a keletkezett joganyag száma, hanem a hatáskör gyakorlójának jogosultsága vagy kötelezettsége tekintetében a rendelkezések összevetése és értelmezése miatt is.

A *honvédelmi célú elektronikus információs rendszer* fogalmát[17] kormányrendelet határozza meg (a rendelet alkalmazásában), az Ibtv.[18] felhatalmazása alapján. Ez az információs rendszer összetett, mivel a honvédelemért felelős miniszter vezetése, irányítása alatt álló szervek zárt célú elektronikus információs rendszereit, valamint egyéb – funkciója, rendeltetése, feladatellátása szerint – nyílt elektronikus információs rendszereit jelenti. A két információs rendszer összessége támogatja ágazatspecifikus módon a honvédelmi ágazaton belüli és ágazatok közötti működést.

A zárt célú elektronikus információs rendszer a honvédelmi ágazatban is rendeltetése szerint elkülönült. Információs feladatok ellátását biztosítja, és kizárólagosan speciális igények kielégítését szolgálja az e célra létrehozott szervezet útján és működése által. Ilyenek a honvédelmi miniszter vezetése, irányítása alá tartozó szervek és a tulajdonosi joggyakorlása alatt álló gazdasági társaságok használatában lévő zárt célú elektronikus információs rendszerek, többek között a honvédelmi célú közigazgatási döntés-előkészítő és vezetés-irányítási rendszerek, a honvédelmi stacioner és tábori, nemzetközi műveleteket, valamint gyakorlatokat támogató műveleti vezetési rendszerek, a katonai nemzetbiztonsági területen titkos információgyűjtést, illetve titkos adatszerzést támogató rendszerek stb.

Zárt célú elektronikus információs rendszer:
– a Magyar Honvédségnél üzemelő MH Kormányzati Célú Elkülönült Hálózat (katonai és közigazgatási szakfeladatok), amely a honvédelmi szervezetek központi szolgáltatásait látja el (mellette rengeteg helyi rendszer üzemel);
– a KNBSZ[19] elkülönült hálózata;
– a védelmi igazgatási szakfeladatokat szolgáló rendszer;
– a HM tulajdonú gazdasági társaságok saját rendszerei.

A honvédelmi elektronikus információs rendszerekkel összefüggésben ki kell emelni KNBSZ-t, amely a kibertér biztonságával kapcsolatos feladatai ellátása során elemzi és értékeli a működési területén

[17] 187/2015. (VII. 13.) kormányrendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról 1. § 2.
[18] 2013.évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 1. § 47.
[19] Katonai Nemzetbiztonsági Szolgálat

felderített, a nemzetbiztonság katonai elemeit érintő információkat, azokról folyamatosan tájékoztatja a honvédelemért felelős minisztert, a minisztérium feladat- és hatáskörrel rendelkező vezetőit stb.

A honvédelmi ágazatnál (EU terminológiával: szektornál) a kibertér védelmét – zárt célú elektronikus információs rendszerekkel kapcsolatos hatósági, biztonsági felügyeleti feladatok ellátását, továbbá a honvédelmi célú elektronikus információs rendszerek biztonságának felügyeletét – kizárólagosan a KNBSZ látja el. Tehát az ágazatspecifikusságra tekintettel a kibervédelemben a szervezet az, ami jogosult és kötelezett az összetett elektronikus információs rendszerek vonatkozásában, így a kormányrendelet azonos jogszabályhelyeket jelölt meg a feladat ellátásában.

A honvédelmi ágazati eseménykezelésben az azonosított szereplők mellett az Alkotmányvédelmi Hivatal, a KKM és a nemzeti koordinációs feladatokat végző nemzeti kiberkoordinátor említendő még. Az eseménykezelési együttműködés egyben a honvédelmi ágazat nemzeti és nemzetközi szervezetekkel való kapcsolati rendszerét is megmutatja. A KNBSZ szakmai felkészültsége a biztosíték az adott kibervédelmi területű művelet (például egy kód elemzése) vagy stratégia szintű feladat megoldásához szükséges közös kormányzati szintű együttműködéshez (például munkacsoportban egy folyamat kidolgozása, jogszabály előkészítése).

A honvédelmi célú elektronikus információs rendszereket érintő biztonsági események (tehát az elektronikus biztonsági rendszerben változást vagy ismeretlen helyzetet előidéző, nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat stb.) és fenyegetések kezelése a KNBSZ feladata, amelyet a szakmai irányítása és koordinálása alatt álló, szakfeladat szerint elkülönülő – a honvédelemért felelős miniszter irányítása, vezetése alatt álló szervnél, szervezetnél működő – eseménykezelő központokkal együtt lát el.

A magyar eseménykezelés folyamatában a kommunikációs protokoll egyszerű: GovCERT központú, ami azt jelenti, hogy az eseményeket (nemzetközi szakkifejezéssel: incidenseket) a GovCERT felé kell bejelenteni, aki továbbítja a szükséges információkat az összes érintett szervezet felé, rögzíti az esetet, szükség esetén közvetlen együttműködést ajánl fel.

8.1.5.6. BM Országos Katasztrófavédelmi Főigazgatóság

A BM Katasztrófavédelmi Főigazgatóságának a már ismert tűzoltáson és árvízveszélyen kívül fontos feladata van a kibervédelem és kiberbiztonság területén is. 2008-ban jelent meg a kritikus infrastruktúrák azonosításáról és kijelölésükről, valamint ezek védelmi fejlesztéseinek szükségességéről szóló 2008/114/EK tanácsi irányelv. A hazai Zöld Könyv megjelenése után a 1049/2010-es kormányhatározat a belügyminiszter hatáskörébe utalta a nemzeti kapcsolattartó pont feladatait és az európai kritikus infrastruktúrák védelmével kapcsolatos kérdések koordinálását.

A BM OKF Országos Iparbiztonsági Főfelügyelőség tevékenységi körén belül kiemelt helyet foglal el a kritikus infrastruktúra védelmi szakterület, melynek egyik fő tevékenysége a jogalkotási és szabályozási feladatok végrehajtása. Ennek eredményeképpen 2013. március 1. napján hatályba lépett a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény, valamint a hozzá kapcsolódó 65/2013. (III. 8.) általános végrehajtási kormányrendelet. A jogszabály célja egyrészt a létfontosságú rendszerelemek azonosítása, másrészt a kijelölés megtörténte után a megfelelő szintű – humán, fizikai és informatikai – védelem biztosítása.

2013. március 19-én átadták a Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központját (LRLIBEK), amely az Országos Katasztrófavédelmi Főigazgatóság Országos Iparbiztonsági Felügyelőségén működik. Feladata a hálózatbiztonság, valamint az iparbiztonsági események kezelése, gyakorlatok, ellenőrzések koordinálása.

Az LRLIBEK bővíti a hálózatbiztonsági szakmai tevékenységet, valamint szakmai működési protokollt és szabályrendszereket állít fel.

8.1.5.7. A Terrorelhárítási Központ

A Terrorelhárítási Központ feladatát az 1994. évi XXXIV. törvény határozza meg, amely – bár kifejezetten nem tér ki a kiberbűnözésre, hiszen nyomozati jogkört nem gyakorol – a 2012. évi C. törvényben, a Büntető Törvénykönyv 314–316. §-ban taglalt *terrorcselekménnyel* összefüggésben az internet felhasználásával történő szerveződést, terrorsejtek szerveződését, az ezekkel összefüggésben történő szerveződéseket, csoportokat, személyeket deríti fel és figyeli meg. Továbbá hatáskörébe tartozik egyes kritikus infrastruktúrák vagy az azokon kívüli kiemelt létesítmények – akár azok informatikai rendszereinek – védelme, az ellenük történő támadás megakadályozása, felderítése.

Ugyanakkor nem rendelekezik nyomozati jogkörrel, így a törvényben előírt tevékenysége során az Rtv. 7/F. §-a alapján együttműködik a rendőrséggel, valamint a magyar és külföldi titkosszolgálati szervezetekkel is.

8.1.6. Büntető törvénykönyvi tényállások

Informatikai környezetben szinte minden bűncselekmény elkövethető,[20] de az állami és önkormányzati szervek sérelmére vagy működésükkel összefüggésben nagyobb valószínűséggel előforduló bűncselekmények alap tényállása egy rövid ismertetést tesz indokolttá.

8.1.6.1. Btk. 375. § Információs rendszer felhasználásával elkövetett csalás

Aki jogtalan haszonszerzés végett információs rendszerbe adatot visz be, vagy az abban kezelt adatot megváltoztatja, törli vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz, bűntettet követ el. A tényállás első része a haszonszerzés végett végrehajtott, azaz célzatos cselekményeket foglalja magában.

A bűncselekmény által védett jogi tárgyak a számítástechnikai rendszer integritásához fűződő jogi érdeket, vagyoni viszonyokat, és az elektronikus készpénz-helyettesítő fizetési eszközök forgalmának a biztonságát védik.

A bűncselekmény elkövetési tárgya maga a számítógépes adat.

A bűncselekmény elkövetési formái:

Az elektronikus adat bevitele. Ez történhet offline, vagy akár online módon is. Ennél a deliktumnál hiányoznak a klasszikus értelemben vett tényállási elemek, a tévedésbe ejtés vagy a tévedésben tartás. A kárt az információs rendszer jogtalan befolyásolása okozza, azáltal, hogy az elkövető az információs rendszerbe bármilyen valótlan adatot bevisz, vagy egy adathordozóról (például CD-ről, DVD-ről, Pendrive-ról) feltölt. A már bevitt adat tartalmát az elkövető megváltoztatja műszaki úton. Törléssel az adatot visszavonhatatlanul megsemmisíti.

A Btk. büntetni rendeli a hozzáférhetetlenné tételt is, amikor az adat megszerzésére, kezelésére jogosult személy – akár csak ideiglenesen is – gátolva van az adat elérhetőségében.

Ugyancsak bűncselekményt követ el az, aki például az adatot jogosulatlanul többszörözi.

A *bankkártya-hamisítás* a hamis, hamisított vagy jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz felhasználásával vagy az ilyen eszközzel történő fizetés elfogadásával történő károkozás. Készpénz-helyettesítő fizetőeszköznek minősül a csekk, a hitelkártya, a csekkkártya, a bankkártya (debit- és hitelkártya), a kereskedelmi kártya, a váltó, a Széchenyi Pihenő Kártya

[20] Például a garázdaság vagy a szexuális kényszerítés bűncselekmények természetesen nehezebben, de a hozzájuk kapcsolódó előkészületi, bűnsegédi magatartás nagyon könnyen.

(SZÉP-kártya), az Erzsébet-utalvány, továbbá a takarékbetétkönyv vagy az ilyen betétről kiállított más okirat és elnevezésétől függetlenül minden más, az előzőekkel azonos rendeltetésű okmány.

Jogosulatlan a fizetőeszköz megszerzése, ha azt az elkövető lopással (akár fizikailag veszi magához a bankkártyát vagy pedig erre készített eszközzel megszerzi az azon szereplő adatokat) vagy erőszakkal, fenyegetéssel, megtévesztéssel, illetőleg más jogellenes módon veszi birtokba.

Informatikai környezetben a bankkártyák felhasználása, használata:

- ATM-en (Automatic vagy Automated Teller Machine) keresztüli készpénzfelvétel, lekérdezés, befizetés, feltöltés stb.;
- POS terminálon keresztül történő áruvásárlás vagy szolgáltatás kiegyenlítése;
- virtuális térben interneten történő áruvásárlás vagy szolgáltatás kiegyenlítése (elektronikus vagy online kereskedelem).

A hamis, hamisított, vagy a jogosulatlanul használt bankkártyával történő fizetés elfogadása akár valóságos, akár virtuális térben delictum sui generis fizikai bűnsegéd.

Az interneten a hamis, hamisított kártyák elfogadása tipikusan pénzmosásra utalhat.

A bűncselekmény elkövetője bárki lehet. Az ilyen, az csak szándékosan, pontosabban egyenes szándékkal elkövethető bűncselekmény lehet.

A bűncselekmény sértettje lehet természetes és jogi személy és tipikusan az, akinél a kár keletkezik.

A számítástechnikai bűncselekmények jellemzőit, a kibertér sajátosságait és az elkövetők felkészültségét figyelembe véve látható, hogy a nyomozó hatóság különösen nagy kihívással áll szemben egyes bűncselekmények, így például a gyermekpornográfia, a rosszindulatú támadások esetében, amelyek mind Európai Unión belüli, mind pedig globális, unión kívüli összefogás nélkül nem számolhatók fel.

Az összefogás, a rendszeres tapasztalatcsere megvalósulása mind nemzeti, mind pedig nemzetközi/tagállami szinten megvalósul.

8.1.6.2. Btk. 423. § információs rendszer vagy adat megsértése

Aki információs rendszerbe az annak védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad, vétséget követ el.

Aki az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz, bűntettet követ el.

A paragrafus (1) bekezdésének jogi tárgya a számítástechnikai rendszerek integritása, biztonsága.

A tényállás további jogi tárgyai: az (1) bekezdés *b)* és *c)* pontjában e rendszerek biztonságos működése, *c)* pontjában az előzőek kiegészülnek az elektronikus adatok megbízhatóságához, hitelességéhez fűződő érdekkel, valamint tartalmától függően az azok által megtestesített értékkel.

A bűncselekmény *elkövetési tárgyai:* a számítógép vagy számítástechnikai rendszer és a számítógépes programok és elektronikus adatok.

Egy informatikai hálózat lehet belső hálózat (intranet), az internet részét képező hálózat (például egy bank vagy biztosító hálózata), de hálózat a szerver feltalálási helye a valós térben vagy a virtuális térben (mint például az úgynevezett cloud-szerverek esetében). A hálózatok egy része publikus, azaz minden felhasználó által, céljának megfelelően használható, másik részük azonban a nyilvánosság elől elzárt, és csak a beavatottak által ismert jelszóval, egyéb azonosítóval használható.

A jogosulatlan belépés

Ez történhet egy más által jogszerűen birtokolt, használt számítástechnikai rendszerbe, úgy, mintha az támadó a jogosult felhasználó lenne (színlelés) vagy történhet számítástechnikai rendszeren keresztül egy védett hálózatba.

Szükséges, hogy a számítógép vagy a számítógépes, számítástechnikai hálózat valamilyen biztonsági, védelmi megoldással aktívan védve legyen. Az aktív védelem – a tényállás szerint – azt jelenti, hogy a belépéshez felhasználónév, jelszók vagy valamilyen azonosító használata legyen szükséges.

Így ez azt jelenti, hogy aki jogosulatlanul belép, az az aktív védelemmel ellátott számítógépet vagy számítástechnikai rendszert vagy védett hálózatot a jogosultsága kereteit túllépve használja. Az informatikai rendszer vagy hálózat biztonsági rendszerhiányosságainak kihasználásával lép be jogosulatlanul, vagy a jogosult felhasználó nevével (belépési kódjával), az általa használt jelszóval vagy a belépést biztosító adattal lép be.

Ugyanakkor a bűncselekmény elkövetése szempontjából lényegtelen, hogyan jut a támadó a belépéshez szükséges adatokhoz (megtévesztéssel, más csalárd módon, kifürkészéssel, a felhasználó hanyagsága folytán – a tipikus példa a monitoron vagy munkaasztalon hagyott felhasználónév és jelszó kombinációja –, kódfejtő program segítségével); a megszerzés módja irreleváns Ugyanakkor, amennyiben azokat a jelszavakat fizikai erőszak, fenyegetés alkalmazásával szerzik meg, akkor már a kényszerítés tényállása állapítható meg.

A belépés nem jogosulatlan, amennyiben a számítástechnikai rendszer nem védett, illetve a védelem nem aktivált.

A belépési jogosultság kereteinek túllépése, illetőleg annak megsértése

Az elkövető a saját felhasználónevével, jelszavával, az engedélyezett belépési ponton lép be az információs rendszerbe, ám a felhasználói jogosultságát meghaladó műveleteket kíván folytatni. Például a felhasználó jogszerűen veszi igénybe a kereskedelmi bankok telebanking szolgáltatását, de olyan műveleteket kíván végrehajtani, amelyre a bankkal kötött szerződésben biztosított hozzáférés jogosultsága már nem terjed ki (például másik személy vagy vállalkozás bankszámláját kívánja megtekinteni).

Hasonló minősítésű az a cselekmény, ha a rendszergazda – jogellenesen – az intézmény, vállalkozás felhasználóinak adatait kigyűjti.

A tényállásban kiemelt „akadályozáshoz” rosszindulatú, kártékony programokat, úgynevezett malware-eket telepítenek, aktiválának. A vírus, féreg, logikai bomba és más programok alkalmasak az információs rendszerek működésének megzavarására, vagy azok a kezelt elektronikus adatokat, akár a számítógépet, hálózatot vezérlő programokat támadják. Ezek a számítástechnikai rendszer működésének „lassulása”, a felhasználó akaratától függetlenül fájlok, könyvtárak törlődése vagy újak megjelenése, a számítógép szabad memóriájának indokolatlan fogyása, telítődése, egyes programok hibás működése, a számítógép leállása és más káros folyamatok révén észlelhetők. A malware-ek feltöltése a rendszerbe történhet offline módon mint célzatos a bűncselekmény (például külső adathordozóval vagy közvetlenül a számítástechnikai rendszerbe juttatva), de akár illegálisan vagy épp legálisan letöltött programmal is telepíthetők közvetlenül a rendszerbe.

Érdekes, hogy maga a sértett is közreműködhet malware-ek elhelyezésében, amikor például a felhasználó nem megbízható helyet (például szex-oldalt) látogat, és szándéktalanul tölti le a malware-t, vagy illegálisan programot, filmet akar letölteni, ami ugyancsak tartalmazza a malwaret is. Ha a felhasználó a vírusvédelmet egyáltalán nem vagy nem kellő gondossággal választja ki, a malware így is fel tud települni. Ha a rendszer rendelkezik ugyan megfelelő, legális szoftverekkel, ugyanakkor ezek frissítését nem végzik el, úgy nem biztos, hogy felismeri az újabb típusú rosszindulatú szoftverek támadását.

Ezek alapján felvethető a felhasználó felelőssége, hogy megtesz-e mindent számítógépe védelmében.

Előrefordulhat, hogy nem offline módon, hanem interneten keresztül, illegális letöltő oldalakról jut el a malware a felhasználó eszközére, rendszerébe. Ez nemcsak az illegális letöltő oldalakról juthat el a rendszerbe, hanem fertőzött e-mailen keresztül vagy weboldalakról letöltött tömörített fájlokban, akár a „.exe" kiterjesztéssel, illetve linkekre kattintva aktiválhatók (például a trójai vírusok is ilyen módon töltődnek le).

Az online térben a malware *első feltöltése* tipikusan szándékos cselekmény, hiszen akár hacking (elektronikus betörés) útján, akár a weblapon, P2P hálózaton megosztva terjeszti a malware-t, az elkövető szándéka az, hogy az eljusson más felhasználók gépére is. Ugyanakkor annak a felhasználónak a bűnössége, aki továbbadja azt a programot, amelybe egy malware-t csomagoltak, már lehet szándékos vagy gondatlan, de akár vétlen is.

Az áldozattá válás véletlenszerű. Bárki letöltheti a malware-t, és a letöltők egy része aktiválja is azt (például kibontja a tömörített fájlt).

Ugyanakkor léteznek olyan malware-k, amelyeknek a hatása egyedi, ilyen volt a Stuxnet illetve a Duqu is.

Az információs rendszerben lévő adat (elektromos impulzus) változtatása, törlése, hozzáférhetetlenné tétele

Az elektronikus adatok megváltoztatása és törlése történhet a rendszerbe vagy egyetlen számítógépbe történő jogszerű és jogellenes belépést követően, vagy malware offline vagy online feltöltésével.

Az „információs rendszerben levő" adat lehet egy program (software) mint elektromos impulzusok meghatározott, logikai sorrendje. A *program módosítása* (bármely elemének megváltoztatása) a rendszer működésének akadályoztatását is jelenti.

Az *elektronikus adat megváltoztatása* gyűjtőfogalom, amely az adat tartalmának bármilyen módon történő módosítását jelenti. Ez felöleli az elektronikus adat felülírásán, kiegészítésén túl annak részleges törlését is, hiszen ez utóbbi is az adat tartalmának módosítását jelenti.

Nemcsak a számítógép memóriájában tárolt adatok tartalma módosítható, hanem akár az adathordozón tárolt adatoké is. Ugyanakkor, amennyiben az adatot csak részlegesen törölték vagy tették hozzáférhetővé, a bűncselekmény ugyanúgy megvalósul mindkét esetben! Ha az arra nem jogosult személy az adat vagy az azt tartalmazó könyvtár hozzáférhetővé tételét olyan új jelszó vagy elérési útvonal megadásával oldja meg, amelyet a jogosult nem ismer, vagy akár magát a külső adathordozót fizikailag rejti el, a bűncselekmény még így is kivitelezhető.

A bűncselekmény egyik minősített esete, amikor az elkövető több informatikai rendszerbe tör be, és „megfertőzi" azokat a rosszindulatú programokkal.

A másik eset, az úgynevezett terheléses vagy túlterheléses támadás („DoS- vagy (D)Dos – denial of service – támadások) végrehajtása. Ennek során a támadó sok száz vagy több ezer felhasználó gépeinek felhasználása révén kísérel kapcsolatot létesíteni a támadott számítógéppel. A sok száz vagy esetleg ezer úgynevezett „zombi" számítógép hálózattá, az úgynevezett bot-netté (robot-network – robot hálózat) áll össze, amelyet a támadó számítógépe vezérel. Az egyszerre küldött nagy mennyiségű adatkérés és -továbbítás bénítja a támadott számítógépet és rajta keresztül az információs rendszert. Az úgynevezett botnetet létrehozó programok általában az illegálisan letöltött programokban rejtőznek, amelyeket a felhasználók az általuk kívánt programmal együtt telepítenek a gépükre, anélkül, hogy tudnának róluk.[21]

Az informatikai környezetben elkövetett bűncselekmények esetében a sértettek száma eltérhet az online és az offline módnál, de nem minden esetben. A sértettek száma a rosszindulatú programot letöltők számától függ.

[21] Nagy Zoltán András: *Az új számítógépes bűncselekményekről.* http://www.mabie.hu/index.php/cikkek-tanulmanyok/95-dr-nagy-zoltan-az-uj-szamitogepes-buncselekmenyekrol-hatter-es-elemzes (a letöltés ideje: 2017. március 30.)

8.1.6.3. Btk. 424. § információs rendszer védelmét biztosító technikai intézkedés kijátszása

Aki a 375. §-ban, a 422. §-ban vagy a 423. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez vagy forgalomba hoz, illetve jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja, vétséget követ el.

Az információs rendszer védelmét biztosító technikai intézkedés kijátszásának bűncselekménye az információs rendszer vagy adat megsértésének és az információs rendszer felhasználásával elkövetett csalásnak az előkészülete.

Ezzel a szabályozással a jogalkotó az informatikai rendszerbe való jogosulatlan vagy a jogosultság kereteit túllépve a belépést lehetővé tevő (illegális) program, jelszó, belépési kód, más adat készítését, mások számára hozzáférhetővé tételét bünteti, hisz ezek által a védett rendszerek feltörhetők. A védett számítástechnikai rendszerekbe történő jogosulatlan belépés teszi lehetővé a rendszer és az adatok elleni legkülönfélébb bűncselekmények elkövetését.

A bűncselekmény jogi tárgya az elektronikus adatfeldolgozás és -átvitel integritása, biztonsága, mely magában foglalja a számítástechnikai rendszert és annak működését, valamint a feldolgozásra rendelt adatok mint elektronikus impulzusok biztonságát.

A deliktum elkövetési tárgya az elektronikus adatfeldolgozó és -átviteli rendszer védelmi-biztonsági megoldásainak kijátszására alkalmas program, belépési kód, jelszó vagy egyéb adat, amely a védett rendszerbe történő jogszerű belépést biztosítja. *Belépési kód* a felhasználónév, amely a hozzárendelt jelszóval együtt lehetővé teszi valamely hálózatba, számítógépbe a belépést a jogosult számára. A *jelszó* a hálózat (internet, intra- és extranet), valamint az adatállomány hozzáféréséhez szükséges azonosító kulcsszó. Általában jelszavak védik a BIOS-t, különböző operációs rendszerekben például a megosztott erőforrásokat, a szövegszerkesztő programokban a dokumentumokat stb.

A bűncselekmény elkövetési magatartásai: valamely védett elektronikus informatikai rendszerbe történő jogosulatlan belépést biztosító program, jelszó, belépési kód, vagy számítástechnikai rendszerbe való belépést lehetővé tevő adat megszerzése, módosítása, készítése. Készítés alatt a jogalkotó a program írását, az adott elektronikus információs rendszer védelmére szolgáló jelszó generálását, a jelszó felülírását stb. érti. Átadás a belépést biztosító eszköznek az adott számítástechnikai rendszer vonatkozásában a program készítőjétől különböző személynek a birtokába adása. Közömbös, hogy ez ingyenesen, visszterhesen, megtévesztéssel vagy más módon történt. A megszerzés módja legfeljebb büntetéskiszabási szempontként értékelhető. A *hozzáférhetővé tétel* a program, a jelszó, az adat megadása valamilyen módon, akár aktív, akár passzív magatartással (például többek által használt helységben, irodában, gépteremben a belépési kód, jelszó stb. asztalon, képernyőre ragasztott papírdarabon történő otthagyása). A *forgalomba hozatal* révén több személy számára hozzáférhetővé teszik a feltörésre alkalmazható programot.

A *rendelkezésre bocsátás* a számítástechnikai program, jelszó, belépési kód, vagy valamely számítástechnikai rendszerbe való belépést lehetővé tevő adat készítésére vonatkozó gazdasági, műszaki, szervezési ismeret átadása másnak, illetve kódfeltörő program írásához, jelszógeneráláshoz, ezek megszerzéshez, forgalomba hozásához szükséges elméleti vagy gyakorlati ismeretek, programrészletek továbbadása, kapcsolatrendszer megosztása. Nem tartozik ide ilyen programoknak a szakirodalomban történő megnevezése, a program működésének, hatásmechanizmusának leírása.

Nem büntethető az, aki program-, jelszó- vagy adatkészítő tevékenységét a hatóság előtt felfedi, és az elkészített dolgot a hatóságnak átadja, valamint lehetővé teszi a készítésben részt vevő más személyek kilétének megállapítását.

A büntethetőséget megszüntető ok akkor jöhet szóba, ha a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő számítástechnikai programot, jelszót, belépési kódot vagy valamely számítástechnikai rendszer egészébe vagy egy részébe való belépést lehetővé tevő adatot az elkövető azelőtt hozza a hatóság tudomására vagy adja át a hatóságnak stb. mielőtt annak erről ismerete lett volna.

A bűncselekmény elkövetője bárki lehet, a szakismeret, a tudás szintje a büntetéskiszabási szempontjából lehet releváns.

A bűncselekmény célzatos, emiatt csak egyenes szándékkal (dolus directus) valósítható meg.

Az IKT rendszerek üzemeltetésével összefüggésben számos esetben merül fel a tárolt, továbbított adatok tartalmával kapcsolatos jogsértés is.

8.1.6.4. Btk. 204. § gyermekpornográfia

Aki tizennyolcadik életévét be nem töltött személyről vagy személyekről pornográf felvételt megszerez vagy tart, készít, kínál, átad vagy hozzáférhetővé tesz, forgalomba hoz, azzal kereskedik, illetve ilyen felvételt a nagy nyilvánosság számára hozzáférhetővé tesz bűntettet követ el.

8.1.6.5. Btk. 385. § szerzői vagy szerzői joghoz kapcsolódó jogok megsértése

Aki másnak vagy másoknak a szerzői jogról szóló törvény alapján fennálló szerzői vagy ahhoz kapcsolódó jogát vagy jogait vagyoni hátrányt okozva megsérti, vétséget követ el.

Vétség miatt büntetendő, aki a szerzői jogról szóló törvény szerint a magáncélú másolásra tekintettel a szerzőt, illetve a kapcsolódó jogi jogosultat megillető üreshordozó díj, illetve reprográfiai díj megfizetését elmulasztja.

A bűncselekmény jogi tárgya a szerzői jogi védelem alá tartozó alkotásokhoz fűződő vagyoni jogviszonyok, azaz az irodalmi, a tudományos és a művészeti alkotások szerzőinek és a kapcsolódó jogi teljesítmények jogosultjainak önálló jogai.[22] Mivel továbbra is megmaradt ez a tényállás keretdiszpozíciónak, így azt az 1999. évi LXXVI. törvény a szerzői jogról szóló törvény (továbbiakban: Szjt) tölti ki tartalommal.

A korábbi szabályozáshoz képest, amíg az eddig hatályos szerzői jogok megsértése esetében a sértettek számához igazodik a rendbeliség, a különböző jogosultak sérelmére, de egy akarategységben történik meg az elkövetés, úgy most az egyes sértetteknek okozott vagyoni hátrányok összeadódnak, és ez alapján lesz a deliktum minősítve. Vagyis a büntetendőséget értékhatárhoz köti.[23]

A szerzői joggal kapcsolatos bűncselekmények közül említést érdemel a szoftverhamisítás. Ez egy „speciálisan" elkövetett szerzői jogi jogsértés, lévén, hogy a szoftverek esetében (kivéve a freeware) már a magáncélú letöltés is bűncselekménynek számít. Itt a most már hatályos büntető törvénykönyv szerint, amennyiben a szoftver értéke nem haladja meg a 100 ezer forintot, úgy csak szabálysértés elkövetéséről beszélhetünk. Viszont az is tény, hogy akár egy szoftverrel is el lehet követni deliktumot, amennyiben annak forgalmi értéke meghaladja a szabálysértési értékhatárt. Itt újabb probléma merül fel, mert a jogalkotó számára – ahogy fentebb már volt róla szó –„a büntetőjog mint végső eszköz szempontjából indokolatlannak tűnik a nem jelentős mennyiségű szerzői mű vagy kapcsolódó jogi teljesítmény vonatkozásában megvalósuló, személyes célokat szolgáló felhasználások tömeges kriminalizálása. A szerzői jog területén fennálló nemzetközi kötelezettségeink, így különösen a TRIPS egyezmény csupán a szándékos és a kereskedelmi mértékű »szerzői jogi kalózkodásra« *nézve teszi kötelezővé a büntetőjogi szankciók előírását, a kereskedelmi mértéket el nem érő cselekmények esetén nincs olyan körülmény, amely ezen a területen a nemzetközi normáknál szigorúbb büntetőjogi szabályozást indokolná.'*[24]

[22] 2012. évi C. törvény 385.§ Miniszteri Indoklása
[23] 2012. évi. C. törvény 385. § (4) bekezdése
[24] 2012. évi C. törvény 385. § miniszteri indoklása

8.1.6.6. Btk. 386. § védelmet biztosító műszaki intézkedés kijátszása

Aki a szerzői jogról szóló törvényben meghatározott hatásos műszaki intézkedést haszonszerzés végett megkerüli, vétséget követ el.

Vétség elkövetése miatt büntetendő, aki a szerzői jogról szóló törvényben meghatározott hatásos műszaki intézkedés megkerülése céljából az ehhez szükséges eszközt, terméket, számítástechnikai programot, berendezést vagy felszerelést készít, előállít, átad, hozzáférhetővé tesz, vagy forgalomba hoz, illetve az ehhez szükséges vagy ezt könnyítő gazdasági, műszaki vagy szervezési ismeretet másnak a rendelkezésére bocsátja.

Az itt felsorolt büntető törvénykönyvi tényállásokhoz számos minősített eset és részletszabály kapcsolódik, de ökölszabályként kijelenthető, hogy vélelmezett jogsértés esetén a feljelentés megtétele indokolt, és majd a nyomozó hatóság, illetőleg az ügyészség dönt annak kérdésében, indokolt-e nyomozás elrendelése.

8.1.7. A büntetőeljárásra vonatkozó egyes szabályok

Akár a nyomozó hatóság saját észlelése, akár bejelentés, feljelentés alapján indul is az eljárás, az állami és önkormányzati szervek szempontjából a rendőrség részéről történő kapcsolat felvétel az alábbi klasszikusnak nevezhető formákban ölt testet: megkeresés, lefoglalás, házkutatás.

Ezekhez kapcsolódik még a téma szempontjából speciálisan az információs rendszerben tárolt adatok megőrzésére kötelezés, valamint az elektronikus hírközlő hálózat útján közzétett adatok ideiglenes hozzáférhetetlenné tétele. E kettő felfogható egyfajta speciális megkeresésnek is, abban az értelemben, hogy a nyomozó hatóság a címzettet valamilyen tevékenységre hívja fel.

Ez a leírás jellemzően az eljárás eredményes lefolytatása és az arányosság szempontjából egy alkalmazhatósági sorrendet is mutat.

Ha csak egy bizonyos információra van szükség, amelynek szolgáltatására az állami, önkormányzati szerv egyébként is köteles, és az információ kinyeréséhez nem szükséges speciális ismeret, akkor a nyomozó hatóságok a megkeresés eszközéhez nyúlnak, azaz küldenek egy átiratot. Erre példa lehet annak lekérdezése, hogy adott időszakban mely munkatársak végeztek munkát az állami, önkormányzati szerv adott épületében.

Ha a beszerzendő információ az eljárás szempontjából kiemelten fontos, vagy annak kinyeréséhez speciális információ szükséges, esetlegesen tartani lehet attól, hogy az adatokat törlik vagy felülírják, akkor egy erőforrás-igényesebb és gyorsabb eljárási cselekmény következhet: a lefoglalás. Erre példa lehet, amikor a nyomozó hatóság akár az állami, önkormányzati szerv épületében önálló cselekményként, akár egy nyilatkozattételre jogosult személy tanúkénti kihallgatása alkalmával lefoglalja a munkatársak rendszerhasználatáról szóló logfájlokat tartalmazó adatokat és az azokat rögzítő adathordozót.

A házkutatás az eljárás alá vont személy jogaiba történő legerősebb beavatkozás az itt említettek közül. Tipikusan akkor alkalmazható, ha az előbbi kettő intézkedés nem biztos, hogy eredményre vezetne, vagy a nyomozás érdekében ez tűnik a legcélszerűbbnek. Jellemzően akkor kerül foganatosításra, ha az eljárás alá vont személy nem együttműködő, vagy a beszerzendő adat, információ nem egyszerűen körülírható, annak kigyűjtéséhez speciális ismeret szükséges. Példaként jelölhető, amikor az állami, önkormányzati foglalkoztatott a hivatali informatikai eszközöket használja fel illegális tevékenységre például zsaroló, fenyegető e-mailek küldésére, gyermekeket ábrázoló pornográf felvételek tárolására.

8.1.7.1. Megkeresések

A Be. 71. § rendelkezései szerint a bíróság, az ügyész és a nyomozó hatóság állami és helyi önkormányzati szervet, hatóságot, köztestületet, gazdálkodó szervezetet, alapítványt, közalapítványt és társadalmi

szervezetet kereshet meg tájékoztatás adása, adatok közlése, átadása, illetőleg iratok rendelkezésre bocsátása végett, és ennek a teljesítésére legalább nyolc, legfeljebb harminc napos határidőt állapíthat meg.

Bizonyos esetekben a megkereső kérhet sürgős vagy azonnali teljesítést is, de a Be. alapján ez nem kikényszeríthető a megkeresettektől. Ha azonban a megkeresett a kérés ellenére nem teljesíti sürgősséggel a megkeresést, úgy a nyomozó hatóság törvényesen járhat el, ha a kért információt lefoglalás vagy házkutatás – mint kényszerintézkedés – útján szerzi be.

A megkeresés jogintézménye az igazságszolgáltatás eredményes és gyors működéséhez elengedhetetlen. A gyakorlat szerint a legtöbb megkeresést a nyomozó hatóságok küldik ki.

A törvény a megkeresés formájáról nem rendelkezik, de elsősorban írásban, legtöbbször egyszerű átirat formájában történik, de gyakori a szóban, távbeszélőn vagy más módon, telefax, e-mail útján közölt megkeresés is.

A rejtjelezett vagy más módon megismerhetetlenné tett adatot a megkeresett köteles az átadás vagy a közlés előtt eredeti állapotába visszaállítani, illetőleg a megkereső számára az adat tartalmát megismerhetővé tenni.

A megkeresett szerv köteles az adatszolgáltatást – amely magában foglalja az adat feldolgozását, írásban vagy elektronikus úton való rögzítését és továbbítását is – térítésmentesen teljesíteni.

A megkeresett a megállapított határidő alatt – ha törvény másképp nem rendelkezik – köteles a megkeresést teljesíteni, vagy a teljesítés akadályát közölni.

Ha a megkeresés személyes adatok közlésére vonatkozik, az csak annyi és olyan személyes adatra vonatkozhat, amely a megkeresés céljának megvalósításához elengedhetetlenül szükséges. A megkeresésben az adatkezelés pontos célját és a kért adatok körét meg kell jelölni. A cél ebben az értelemben természetesen nem azt jelenti, hogy a kérdéses adatokra az eljárás során milyen feltevés bizonyítására van szükség, csupán annyit, hogy mely ügyszámon, milyen bűncselekmény miatt folyó eljárásban van azokra szükség.

Ha a megkeresés eredményeként olyan személyes adat jut a megkereső tudomására, amely a megkeresés céljával nem függ össze, az adatot törölnie kell a megkeresőnek, és azt az ügyiratban nem tarthatja meg. Személyes adatnak minősül a meghatározott természetes személlyel kapcsolatba hozható adat, és az adatból levonható, az érintettre vonatkozó következtetés.

Ha a megkeresett szerv a megkeresést a megállapított határidőn belül nem teljesíti, vagy a megkeresés teljesítését jogosulatlanul megtagadja, rendbírsággal sújtható, de ehhez mindenképpen fontos a megkereső számára, hogy a megkeresés megküldését és annak címzetthez megérkezését igazolja. E-mail esetén ez jellemzően nem teljesülhet, ezért a jelenlegi gyakorlatban az kevésbé használt. Akadályként az is említhető, hogy a nyomozásokat lefolytató személyek – az ügy előadói – sok esetben nem rendelkeznek publikus internetes e-mail-címmel, csak intranetes e-mail-címmel.

A rendbírság kiszabásának indoka nemcsak az lehet, ha a megkeresett nem válaszol, hanem az is, ha annak csak részben vagy a megszabott határidőn túl tesz eleget.

8.1.7.2. A lefoglalás

A Be. 151. § értelmében a lefoglalás a bizonyítás érdekében vagy az elkobzás, illetőleg a vagyonelkobzás biztosítására a dolognak a bíróság, az ügyész, illetőleg a nyomozó hatóság általi őrzésbe vétele vagy megőrzésének más módon történő biztosítása.

A bíróság, az ügyész, illetve a nyomozó hatóság elrendeli annak a dolognak, információs rendszernek, vagy abban tárolt adatokat tartalmazó adathordozónak vagy adatnak a lefoglalását, amely bizonyítási eszköz, illetve a törvény értelmében elkobozható, vagy amelyre vagyonelkobzás rendelhető el.[25]

[25] 2017. április hónapján elérhető legújabb Be. Tervezet T/13972. számú törvényjavaslat 308. § (3) bekezdés szerint „Lefoglalni az ingó dolgot, a számlapénzt, az elektronikus pénzt vagy az elektronikus adatot lehet."

A lefoglalás tehát olyan kényszerintézkedés, amely a birtokosnak, a tulajdonosnak a birtokláshoz és a tulajdonhoz való jogát korlátozza a bizonyítás, az elkobzás és a vagyonelkobzás biztosítása érdekében.

A büntetőeljárás sikerének biztosításához elengedhetetlen, hogy a hatóság felkutassa és megszerezze a bűncselekmény elkövetését bizonyító bizonyítási eszközöket, illetve azokat a dolgokat, amelyek elkobozhat,[26] vagy azt a vagyont és mindazt, amire a vagyonelkobzás elrendelhető. Ennek értelmében a lefoglalás tárgya ingó és ingatlan dolog, állat és növény is lehet, de témánkhoz sokkal szorosabban kapcsolódik, hogy lehetnek azok az informatikai rendszerhez kapcsolódó vagy informatikai úton rögzített adatok is. A tárgyi bizonyítási eszközhöz tartozik, és a lefoglalás tárgya lehet az irat, a rajz és minden olyan tárgy, amely műszaki, vegyi vagy más eljárással adatokat rögzít. Ahol e törvény *iratról* rendelkezik, ezen az adatot rögzítő tárgyat is érteni kell, tehát a lefoglalni szándékolt adatot nem csak annak átmásolásával foglalhatja le jogszerűen a nyomozó hatóság, hanem az adathordozóval együtt is.

A közjegyzői, ügyvédi irodában és az egészségügyi intézményben, az iratok lefoglalására egyes postai és hírközlési küldemények, valamint a szerkesztőségek sajtótermékeinek a lefoglalására kizárólag a bíróság, illetve egyes esetekben az ügyészség jogosult és ezek foganatosítására is speciális szabályok vannak érvényben.

A házkutatáshoz hasonlóan a lefoglalás érdekében is a dolog, illetve az információs rendszer vagy az ilyen rendszerben tárolt adatokat tartalmazó adathordozó birtokosát vagy az adat kezelőjét fel kell szólítani, hogy a keresett dolgot adja át, illetve az információs rendszerben tárolt adatot tegye hozzáférhetővé. Ha ezt önként nem teszi meg, rendbírsággal sújtható, kivéve a terheltet és azt, aki a tanúvallomást megtagadhatja,[27] továbbá aki tanúként nem hallgatható ki. Az átadás, illetve a hozzáférhetővé tétel megtagadása nem akadálya annak, hogy a keresett dolgot, illetve az információs rendszerben tárolt adatot házkutatással vagy motozással megszerezzék. Erre az érintettet a nyomozó hatóság eljáró tagjának figyelmeztetnie kell.

A lefoglalás a házkutatáshoz hasonlóan, kivételesen halaszthatatlan nyomozási cselekményként is elrendelhető. A lefoglalásról alakszerű határozatban kell rendelkezni, ami ellen jogorvoslattal lehet élni az ügyész, majd a nyomozási bíró felé is.

A lefoglalt dolgokat jegyzőkönyvben vagy más okiratban a mennyiségük, értékük, minőségi állapotuk feltüntetésével, egyedi azonosításra alkalmas módon fel kell sorolnia a jegyzőkönyvet vezető nyomozónak.

A lefoglalt dolgot úgy kell őrizni, hogy az változatlan maradjon, a bűncselekmény esetleges nyomai el ne tűnjenek, a lefoglalt dolgot ne lehessen kicserélni, és az azonossága könnyen megállapítható legyen. Ez információs rendszerek, illetve ilyen rendszerben tárolt adatok esetében különösen sarkalatos kérdés, mivel ezek a jellemzően digitális nyomok olyan módon módosíthatók, hogy a változtatást rátekintéssel nem lehet megállapítani, illetve az esetek egy jelentős részében nem állapítható meg kétséget kizáróan a változtatás időpontja.[28] Az információs rendszernek és az ilyen rendszerben tárolt adatok lefoglalása esetén a kényszerintézkedés lefolytatásának folyamata és a felhasznált eszközök biztosítják a lefoglalt dolgok integritását, megváltoztatatlanságát.

A lefoglalt tárgy, dolog megőrzése az alábbi módokon valósulhat meg: hatósági letétben helyezik, az érintett őrizetében hagyják, egyes szervek (vállalkozók) őrizetében és kezelésében hagyják. Főszabályként a lefoglalt dolgot letétbe kell helyezni, azaz a nyomozó hatóság eljáró tagjai magukkal viszik, és a hatóság bűnjelkamrájában elhelyezik.

---

[26] Btk. 72. § El kell kobozni azt a dolgot, amelyet a bűncselekmény elkövetéséhez eszközül használtak vagy arra szántak, amely bűncselekmény elkövetése útján jött létre, amelyre a bűncselekményt elkövették, vagy amelyet a bűncselekmény befejezését követően e dolog elszállítása céljából használtak, amelynek a birtoklása a közbiztonságot veszélyezteti, vagy jogszabályba ütközik.

[27] Be. 82. § megtagadhatja a terhelt hozzátartozója, az, aki magát vagy hozzátartozóját bűncselekmény elkövetésével vádolná, aki a foglalkozásánál vagy közmegbízatásánál fogva titoktartásra köteles (lelkész, védő, orvos), a médiatartalom-szolgáltatói tevékenységgel összefüggésben (újságírói tevékenység) információt átadó személy kilétének felfedése elkerülésére vonatkozóan.

[28] Mivel a változtatás időpontja is egy digitális adat, amely szintén a módosítás nyoma nélkül változtatható.

A bíróságnak az ügydöntő határozatában (azaz jellemzően az ítéletben) a lefoglalt dologról az érdemi döntéssel együtt kell rendelkeznie, hogy azt kinek rendeli kiadni, vagy elkobzásról, megsemmisítésről stb. dönt.[29] Ezen túlmenően a lefoglalást a bíróság, az ügyész, illetőleg a nyomozó hatóság megszünteti, ha arra az eljárás érdekében már nincs szükség, azaz a lefoglalás feltételei már nem állnak fenn. A lefoglalást meg kell szüntetni, ha a nyomozást megszüntették, illetőleg annak határideje lejárt.[30] A nyomozás szempontjából szükségtelenül fenntartott lefoglalás megalapozhatja a hatóság kárfelelősségét. A lefoglalás megszüntetéséről alakszerű határozatot kell hozni, de a dolog kiadására csak akkor kerülhet sor a nyomozás során, ha a lefoglalás megszüntetéséről rendelkező határozat ellen egyik érdekelt személy sem nyújt be panaszt, vagy az elutasításra kerül.

A törvény értelmében a lefoglalt dolgot első sorban annak kell kiadni, aki a bűncselekmény elkövetésekor a dolog tulajdonosa volt.

Jelen jegyzet írásának időpontjában a büntetőeljárásról szóló törvény újra kodifikálása zajlik. Korántsem biztos, hogy az igazságügy miniszter által előterjesztett javaslatot a parlament változatlan módon fogadja el, és az sem biztos, hogy annak a Magyar Közlönyben megjelenő formája fog hatályba lépni.[31] Az azonban lényeges, hogy a javaslat számos fórumon az itt idézett formában ment keresztül, így sok szakmai szervezet jogalkotási igényét jelzi.

Az új Be. tervezete az elektronikus adatok lefoglalásával kiemelten foglalkozik. Nem tartja elegendőnek, hogy szakmai szabályok határozzák meg a lefoglalás folyamatát, hanem azt törvényi szintre kívánják emelni az egységes végrehajtás érdekében.

Az elektronikus adat lefoglalása

„315. § (1) Az elektronikus adat lefoglalását

a) az elektronikus adatról másolat készítésével,

b) az elektronikus adat áthelyezésével,

c) az azt tartalmazó információs rendszer vagy adathordozó teljes tartalmáról történő másolat készítésével,

d) az azt tartalmazó információs rendszer vagy adathordozó lefoglalásával, vagy

e) jogszabályban meghatározott más módon

lehet végrehajtani.

(2) A fizetésre használt elektronikus adat lefoglalását úgy is végre lehet hajtani, hogy az elektronikus adattal olyan műveletet végeznek, amely az érintettnek az elektronikus adat által kifejezett vagyoni érték feletti rendelkezési lehetőségét megakadályozza.[32]

(3) Az elektronikus adatként létező irat lefoglalására a 313–314. §[33] rendelkezéseit is megfelelően alkalmazni kell.

(4) Az elektronikus adat lefoglalását úgy kell végrehajtani, hogy az a büntetőeljárás céljából szükségtelen elektronikus adatra lehetőleg ne terjedjen ki, illetve az ilyen elektronikus adatot a lefoglalás a legrövidebb ideig érintse.

(5) Az elektronikus adatot tartalmazó információs rendszer vagy adathordozó akkor foglalható le, ha

a) az elkobozható, illetve vagyonelkobzás alá esik,

b) az tárgyi bizonyítási eszközként bír jelentőséggel, vagy

c) a bizonyítás érdekében az abban tárolt, előre meg nem határozható vagy jelentős mennyiségű elektronikus adat átvizsgálására van szükség.

---

[29] A lefoglalt dolog előzetes értékesítésére is van lehetőség gyors állagromlás, értékvesztés esetén, de ez információs rendszerek, ilyen rendszerben tárolt adatok esetében nem jellemző.

[30] Be. 155. § (1) bekezdés

[31] Az 1998. évi XIX. törvény elfogadását, kihirdetést követően, de még a hatálybalépését megelőzően számos alkalommal módosították. Ezt a helytelen jogalkotási folyamatot szokták úgy említeni, mint „amikor a kocsi megelőzi a lovakat”.

[32] Itt a jogalkotó feltehetően a kriptovaluták és a jövőben esetlegesen megjelenő adatokra vonatkozó átfogó leírást alkalmaz.

[33] Az iratok lefoglalására vonatkozó rendelkezések.

(6) Ha ez az eljárás érdekét nem veszélyezteti, információs rendszer vagy adathordozó lefoglalása esetén az elektronikus adattal rendelkezni jogosult kérésére másolatot kell készíteni az általa megjelölt elektronikus adatról." [34]

Az itt leírt 315. § tehát e könyv írásakor nem rendelkezik kötelező erővel, de fontos iránymutatásul szolgál akkor is, ha nem válik hatályossá.

A házkutatásra és lefoglalásra vonatkozó közös szabályok törvényi rendelkezései szerint a házkutatást és a lefoglalást az érintett kíméletével, lehetőleg a napnak a hatodik és huszonnegyedik órája között kell végezni. Biztosítani kell, hogy az intézkedés folytán ne kerüljenek nyilvánosságra a magánéletnek a büntetőeljárással össze nem függő körülményei; kerülni kell a szükségtelen károkozást.

Aki a házkutatást vagy a lefoglalás érdekében tett intézkedést akadályozza, ezek tűrésére kényszeríthető, és − a terhelt kivételével − rendbírsággal sújtható. A terheltet akár testi kényszerrel lehet erre rábírni, míg mindenki más esetében a rendbírság ad erre lehetőséget a nyomozó hatóság számára.[35]

Akár szakértővel, akár szaktanácsadóval is érkezik a nyomozó hatóság a lefoglalást vagy a házkutatást lefolytatni, egy közel egységes metodika van érvényben arra vonatkozóan, hogy az eljárási cselekményt milyen technikai, technológiai folyamat szerint kell lefolytatni.

A kikapcsolt informatikai eszközök lefoglalása egyszerű folyamat, de a működésben lévők lefoglalásához, vagy a hardverek eltávolítása nélküli adatlefoglalásokhoz olyan eszközök szükségesek, amelyek hitelt érdemlően bizonyítani tudják az eljárás későbbi szakaszában az adatok integritását, megváltoztatlanságát.

Ezek írásvédő vagy bitazonos másolat készítésére alkalmas célhardverek.[36]

Sajnos még nem minden rendőri egység rendelkezik olyan speciális adatmentő, adatrögzítő berendezésekkel és szoftverekkel, amelyek nemzetközi sztenderdek és bizonyítványok szerint igazságügyi szakértői feladatokra alkalmasak. Olykor előfordul, hogy a rendelkezésre álló idő szűkössége vagy szabad kapacitás hiánya miatt a központi rendőri szervektől nem tudnak ilyen segítséget kérni, de a fejlesztések ezen a területen is folyamatosak.

Mivel ezek az eszközök meglehetősen drágák, azokat sok esetben a minisztériumi nyilvántartásba vett igazságügyi informatikai szakértők sem tudják megvásárolni.

8.1.7.3. A házkutatás

Ezt a kényszerintézkedést a Be. 149. §-a szabályozza, mely szerint a házkutatás a ház, lakás, egyéb helyiség, az azokhoz tartozó bekerített hely vagy a jármű átkutatása, továbbá az ott elhelyezett információs rendszer vagy ilyen rendszerben tárolt adatokat tartalmazó adathordozó átvizsgálása az eljárás eredményessége érdekében.

Házkutatásnak akkor van helye, ha megalapozottan feltehető, hogy az a bűncselekmény elkövetőjének kézre kerítésére vezet (nem jellemző, hogy ez a pont az állami, önkormányzati szervek ellen elrendelés alapja lehet); lehetőséget ad a bűncselekmény nyomainak felderítésére, esetleg bizonyítási eszköz, elkobozható vagy vagyonelkobzás alá eső dolog megtalálására vezet. Esetünkben jellemzően ez az elrendelés alapja – különösen nyomok, bizonyítási eszközök felderítése szokott célként szerepelni.

Bár a törvény meghatározza a házkutatás lehetséges okait, összességében e kényszerintézkedésnek is az alapvető célja a bűncselekmény bizonyítékokkal alátámasztott felderítése, az elkövető kézre kerítése, de a végső soron, a büntetőeljárás sikeres lefolytatása.

A házkutatást jellemzően nyomozó hatóság rendeli el. Ritkábban előfordul, hogy ezt bíróság vagy az ügyész rendeli el, de a végrehajtás akkor is tipikusan a nyomozó hatóságok feladata.

---

[34] T/13972. számú törvényjavaslat (2017.04.17.)

[35] Be. 161. § A rendbírság ezer forinttól kétszázezer forintig, különösen súlyos vagy ismételt esetben ötszázezer forintig terjed.

[36] Például: www.logicube.com, http://www.cru-inc.com/imagers-and-writeblockers/, https://www.guidancesoftware.com/tableau/hardware (a letöltés ideje: 2017. április 20.)

Lehetőség van határozat nélkül is házkutatást tartani (halaszthatatlan nyomozási cselekmény – Be. 177. §), de ez csak halasztást nem tűrő esetben lehetséges.[37] Ekkor csak jegyzőkönyv készül az eljárási cselekményről, és a határozatot később készítik el. A házkutatás alkalmával azonban a határozatot, azaz az indokot és a jogalapot szóban közölnie kell a nyomozóhatóság eljáró tagjának.

A házkutatást rendszerint annak jelenlétében kell elvégezni, aki az ügyben érintett, vagy akinél a házkutatást tartják.[38] Ha a házkutatáson az érintett, illetőleg a védője, képviselője vagy megbízott hozzátartozója nincs jelen, az érintett érdekeinek védelmére olyan személyt kell kirendelni, akiről alaposan feltehető, hogy a házkutatással érintett érdekeit megfelelően védi. Ez lehet akár a gyanúsított hozzátartozója, ismerőse, szomszédja, de lehet a hatóság által felkért hatósági tanú is, aki érdektelen, és megfelelően képes a házkutatás lefolyásának, illetőleg e kényszerintézkedés alkalmazása során történt események tényszerű tanúsításának az igazolására. Jelenléte nem mindig kötelező, de ha azt az érintett kéri, indítványozza, akkor attól nem lehet eltérni.

A házkutatás lefolytatásának menete:

- a nyomozó hatóság tagjai igazolják magukat, és közlik jövetelük célját.
- A kutatás megkezdése előtt közölni kell a házkutatást elrendelő határozatot az érintett személlyel, és annak egy példányát át kell adni, ami ellen lehetséges panaszt bejelenteni, de ennek nincs halasztó hatálya. A panaszt az eljáró nyomozó hatóságnak kell jelezni, akiknek kötelessége ezt továbbítani a felügyeletet gyakorló ügyész felé, aki 8 napon belül dönt e kérdésben.
- Ha a házkutatás meghatározott dolog vagy információs rendszeren vagy adathordozón tárolt adat megtalálására irányul, fel kell szólítani az érdekeltet, hogy azt adja elő, illetve tegye hozzáférhetővé. Ha ez megtörténik, a házkutatást akkor lehet folytatni, ha gyanú merül fel arra vonatkozóan, hogy a házkutatás során más bizonyítási eszköz, dolog is fellelhető.[39]
- Az egész eljárási cselekményről jegyzőkönyvet kell felvennie a nyomozó hatóság eljáró tagjának, amelyben minden olyan tényt, körülményt, adatot fel kell tüntetnie, amely a büntetőeljárás szempontjából fontos lehet.
- A jegyzőkönyv mellett lehetősége van a nyomozó hatóság tagjainak fénykép, hangés videofelvétel készítésére.
- Az eljárási cselekmény végrehajtása során a nyomozó hatóság tagjai megakadályozhatják, hogy a cselekmény helyszínén illetéktelen személyek megjelenjenek, érintett személyek a helyszínt elhagyják, kommunikáljanak egymással vagy külső személyekkel.
- Ha a házkutatás során a bűncselekmény nyomhordozóinak vagy tárgyi bizonyítási eszközeinek csomagolására kerül sor, a csomagot a házkutatást szenvedő, illetve megbízottja (képviselője) jelenlétében a helyszínen kell lezárni. A lezárást a nyomozó szerv eljáró tagjának és a házkutatást szenvedőnek, illetve megbízottjának (képviselőjének), valamint a hatósági tanúnak az aláírásával és az aláírás időpontjának a feltüntetésével hitelesíteni kell. A hitelesítés megtörténtének, illetve megtagadásának tényét a jegyzőkönyvben rögzíteni kell. Ennek azért van jelentősége, mert például lefoglalt adathordozók változatlanságának biztosítása érdekében az adathordozót a nyomozó hatóság változatlan formában továbbítja a szakértőnek, aki szakvéleményében kitér arra, hogy a vizsgálatának tárgyát változatlan állapotban kapta-e meg.[40]
- A jegyzőkönyvben a házkutatást szenvedőnek, illetve megbízottjának (képviselőjének), illetőleg a lefoglalást szenvedőnek nyilatkoznia kell arra vonatkozóan, hogy a nyomozási cse-

[37] Például akkor, ha egy házkutatás során derül ki, hogy más lakásban is szükséges volna házkutatást tartani, de az eljárás eredményességét veszélyeztetné, ha a nyomozóhatóság tagjai visszatérnének a szolgálati helyükre és órákkal később tartanák meg alakszerű határozattal kezükben a kényszerintézkedést a másik lakásban, amikorra onnét mindent eltűntetett a gyanúsított.

[38] 2017. április hónapján elérhető legújabb Büntető eljárásjogi törvénytervezet (T/13972. számú törvényjavaslat 302. §) a házkutatás kifejezés helyett a kutatás kifejezést használja. A jelenléttel kapcsolatos rendelkezése szerint a kutatást az érintett ingatlan vagy jármű tulajdonosának, birtokosának vagy használójának a jelenlétében kell végrehajtani, ennek hiányában védője, képviselője, megbízottja, vagy független személy kell jelen legyen.

[39] Ha a házkutatást szenvedő személy tud a nyomozóhatóság által lefoglalni szándékolt dologról, de azt elhallgatja, elrejti, akkor felvetődik bűnpártolás elkövetésének gyanúja. (BTK. 282. §)

[40] Ha a lefoglalt bűnjelet a nyomozóhatóság tagjai vizsgálják, akkor is a felbontás idejéről és helyéről tájékoztatják a lefoglalást szenvedőt, aki (vagy képviselője) jelen lehet

lekmény ténye (azaz a határozatban foglaltak ellen), illetve lefolytatásának módja miatt él-e panasszal.

A *házkutatás* fogalma alá nemcsak a ház, a lakás és az ezekhez szorosan tartozó bekerített hely, például a ház udvarán lévő garázs, melléképületek (műhely, kamra) és a bekerített helyen lévő jármű tartozik, hanem az információs rendszerben vagy ilyen rendszer útján rögzített adatok is.

A házkutatás nemcsak a terhelt tulajdonát képező ingatlanra rendelhető el, és nemcsak az általa kizárólagosan használt lakrészekben foganatosítható, hanem ott is, ahol a terhelttel együtt vagy a terhelt nélkül mások is laknak. Az is előfordul, hogy a házkutatás elszenvedője nem azonos az elkövetővel, sőt egyáltalán nem tud a bűncselekmény elkövetéséről, de megalapozottan feltehető, hogy a keresett dolog, tárgy vagy a bűncselekmény nyomai az ő lakásában vagy információs rendszerében lelhetők fel.

Az általános alapfeltétel házkutatás foganatosításához a bűncselekmény elkövetésének alapos gyanúja. További különös feltétel a megalapozott feltevés arra, hogy a házkutatás a bűncselekmény elkövetőjének kézre kerítésére, a bűncselekmény nyomainak felderítésére, bizonyítási eszköz, elkobozható vagy vagyonelkobzás alá eső dolog megtalálására vezet.

Az eljárási cselekmény végrehajtásához a nyomozó hatóság szaktanácsadót[41] és szakértőt[42] is vihet magával a házkutatásra.

A házkutatásról felvett jegyzőkönyvben minden olyan tényt rögzíteni kell, amelynek a bizonyítás szempontjából jelentősége lehet. Erre egy formanyomtatvány áll jellemzően a nyomozó hatóság rendelkezésére, de nem kizáró ok, ha a teljes jegyzőkönyv kézzel íródik.

A közjegyzői, ügyvédi irodában, az egészségügyi intézményben foganatosítandó házkutatás során további speciális szabályokat ír elő a büntetőeljárási törvény.

Érdekes, hogy Európa legtöbb országában a házkutatás elrendelésére legalább ügyészi elrendelés szükséges, de Magyarországon jelenleg a legtöbb esetben ezt az eljáró nyomozó hatóság egyik vezetője írja alá.

Problémaként merülhet fel, hogy a házkutatás során információs rendszer vagy ilyen rendszerben tárolt adatokat tartalmazó adathordozó átvizsgálása során jellemzően e-mailek tartalmának megismerése is történik, ami a levéltitok védelméhez fűződő jogokat sérti, de a magyar szabályozás e tekintetben sem alkalmaz jelenleg többletkritériumokat, garanciákat. A teljes nyomozásra azonban érvényes, hogy azt az ügyész törvényességi kontrollja alatt kell végrehajtani, illetve azt az érintett lehető kíméletével kell lefolytatni.[43]

8.1.7.4. Az információs rendszerben tárolt adatok megőrzésére kötelezés

A 2001. november 23-án Budapesten aláírt számítógépes bűnözésről szóló egyezmény[44] az Európa Tanács tagjai közötti szorosabb egység megteremtésén túlmenően hatással volt a büntető és a büntető-eljárási törvényünkre is. Az egyezmény 16. és 17. cikkében rögzítettek képezik alapját ezen intézkedéseknek.

Az egyes nyomozások során alapvető fontosságú, hogy az adatok tárolását, továbbítását végző kisebb-nagyobb szervezetek (kiszolgálók) azonnal, haladéktalanul és maradéktalanul végrehajtsák

[41] Be. 182. § (1) Az ügyész és a nyomozó hatóság a nyomozási cselekményeknél szaktanácsadót vehet igénybe, ha a bizonyítási eszközök felkutatásához, megszerzéséhez, összegyűjtéséhez vagy rögzítéséhez különleges szakismeret szükséges, illetőleg az ügyész vagy a nyomozó hatóság valamilyen szakkérdésben felvilágosítást kér.

[42] Be. 99–102. § Ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges a bíróság, az ügyész, illetőleg a nyomozó hatóság a szakértői névjegyzékben szereplő igazságügyi szakértőt, illetőleg szakvélemény adására feljogosított gazdasági társaságot, szakértői intézményt, vagy külön jogszabályban meghatározott állami szervet, intézményt, szervezetet, ha ez nem lehetséges, kellő szakértelemmel rendelkező személyt vagy intézményt (eseti szakértő) rendelhet ki szakértőként.

[43] Lásd Be. 158. §

[44] Magyarországon kihirdette a 2004. évi LXXIX. törvény.

a hatóság által elrendelt kényszerintézkedést, ezáltal megakadályozva annak törlését, felülírását addig, amíg a nyomozó hatóság tagjai azokat meg nem vizsgálják vagy le nem foglalják.

Információs rendszerben tárolt adatok megőrzésére kötelezést a Be. 158/A. § szabályozza. A *megőrzésre kötelezés* a bűncselekmény felderítése és a bizonyítás érdekében a számítástechnikai rendszer útján rögzített adat birtokosának, feldolgozójának, illetőleg kezelőjének az információs rendszerben tárolt meghatározott adat feletti rendelkezési jogának ideiglenes korlátozása.

A bíróság, az ügyész, illetőleg a nyomozó hatóság elrendeli annak az információs rendszerben tárolt adatnak a megőrzését, amely bizonyítási eszköz vagy bizonyítási eszköz felderítéséhez, a gyanúsított kilétének, tartózkodási helyének a megállapításához szükséges.

A megőrzésre kötelezett feladatait, konkrét tevékenységét is meghatározza a törvény.

A megőrzésre kötelezett a határozat vele történő közlésének időpontjától köteles a határozatban megjelölt információs rendszerben tárolt adatot változatlanul megőrizni, és − szükség esetén más adatállománytól elkülönítve − biztosítani annak biztonságos tárolását. A megőrzésre kötelezett köteles az információs rendszerben tárolt adat megváltoztatását, törlését, megsemmisülését, valamint annak továbbítását, másolat jogosulatlan készítését, illetőleg az adathoz való jogosulatlan hozzáférést megakadályozni.

A megőrzésre kötelezést elrendelő a megőrzéssel érintett adatot fokozott biztonságú elektronikus aláírással láthatja el. Ha az adat eredeti helyen történő megőrzése az érintettnek az adat feldolgozásával, kezelésével, tárolásával vagy továbbításával kapcsolatos tevékenységét jelentősen akadályozná, az elrendelő engedélyével az adat megőrzéséről annak más adathordozóra vagy más információs rendszerbe történő átmásolásával gondoskodhat. Az átmásolást követően az elrendelő az eredeti adatot tartalmazó adathordozóra és számítástechnikai rendszerre vonatkozóan a korlátozásokat részlegesen vagy teljesen feloldhatja.

Ahhoz az adathoz, amelyet a megőrzésre kötelezés érint, az intézkedés tartama alatt kizárólag az elrendelő bíróság, ügyész, illetőleg nyomozó hatóság, valamint az elrendelő engedélyével az adat birtokosa vagy kezelője jogosult hozzáférni. Arról az adatról, amelyet a megőrzésre kötelezés érint, az adat birtokosa vagy kezelője az intézkedés tartama alatt csak az elrendelő kifejezett engedélyével adhat más részére tájékoztatást.

A megőrzésre kötelezett köteles haladéktalanul tájékoztatni az elrendelőt, ha a megőrzésre kötelezéssel érintett adatot jogosulatlanul megváltoztatták, törölték, átmásolták, továbbították, megismerték, vagy, ha ezek megkísérlésére utaló jelet észlelt.

A megőrzésre kötelezést követően az elrendelő haladéktalanul megkezdi az érintett adatok átvizsgálását, és ennek eredményéhez képest az adatnak az információs rendszerbe vagy más adathordozóra történő átmásolásával az adat lefoglalását kell elrendelni, vagy a megőrzésre kötelezést meg kell szüntetni.

A megőrzésre kötelezés az adatot tartalmazó adathordozó lefoglalásáig, illetve az adat átmásolásáig, de legfeljebb három hónapig tart. Ez megszűnik, ha a büntetőeljárást befejezték. A büntetőeljárás befejezéséről a megőrzésre kötelezettet értesíteni kell.

Előfordul, hogy a számítástechnikai adatok kizárólag egy belső rendszeren vannak, amelyet a munkáltató üzemeltet. Ebben az esetben ezzel a rendszergazdával szemben kell elrendelni a kényszerintézkedést. Az ezt elrendelő hatóság az őrzés biztonságának fokozása érdekében további biztonsági intézkedést épít be, amikor előírja, hogy a megőrzéssel érintett adatot elektronikus aláírással láthatja el.

Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól 2015. évi CCXXII. törvény 1. § 22. pontja szerint fokozott biztonságú elektronikus aláírás: az eIDAS Rendelet 3. cikkének 11. pontja szerinti aláírás.[45]

[45] Az Európai Parlament és a Tanács 910/2014/Eu rendelete 3.cikk 11. „fokozott biztonságú elektronikus aláírás": olyan elektronikus aláírás, amely megfelel az a 26. cikkben meghatározott követelményeknek; 26. cikk: A fokozott biztonságú elektronikus aláírásnak az alábbi követelményeknek kell megfelelnie: a) kizárólag az aláíróhoz köthető; b) alkalmas az aláíró azonosítására; c) olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozzák létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat; d) olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

A jogintézmény létrehozásának az egyik legfőbb indoka, hogy kiterjedt nemzetközi nyomozásokban sok esetben az egyes államok nyomozó hatóságainak jogsegélykérelmet kell küldeni a másik állam nyomozó hatóságai felé, ami több hónapot is igénybe vehet. Ezek az átmeneti időszakok gyakran oda vezettek, hogy a jogsegélykérelem megérkezésekor az adatok már nem voltak fellelhetők. A jogintézmény alkalmazásával az ilyen jellegű problémák csökkenthetők.

8.1.7.5. Az elektronikus hírközlő hálózat útján közzétett adatok ideiglenes hozzáférhetetlenné tétele

Ez a jogintézmény a büntetőeljárási törvényben rögzített kényszerintézkedés, amely a törvény eredeti szövegében még nem szerepelt.[46] Ez tehát egy eljárási cselekmény, amely a tényállás tisztázásáig kíván egy speciális helyzetet hibernálni, amelyről még nem dönthető el kétséget kizáróan, hogy jogellenes vagy sem.

Érdekes tekintettel lenni arra, hogy az eddig ismertetett kényszerintézkedésekkel ellentétben ezt bíróság rendeli el, aminek az a feltehető oka, hogy a jogalkotó is látta azt a veszélyt, hogy a szólásszabadság korlátozására is alkalmas lehet annak kontroll nélküli alkalmazása.

Az adatok lefoglalásával ellentétben itt nem a nyomozás érdekeinek előmozdítása az elsődleges cél, hanem a vélhetően jogsértő állapot megszűntetése, ideiglenes jelleggel.

A Be. 158/B. § szabályozza az elektronikus adat ideiglenes hozzáférhetetlenné tételét, mely az elektronikus hírközlő hálózat útján közzétett adat (e cím alkalmazásában a továbbiakban: elektronikus adat) feletti rendelkezési jog ideiglenes korlátozását, és az adathoz való hozzáférés ideiglenes megakadályozását jelenti.

Ha az eljárás olyan közvádra[47] üldözendő bűncselekmény miatt folyik, amellyel kapcsolatban elektronikus adat végleges hozzáférhetetlenné tételének[48] van helye, és ez a bűncselekmény folytatásának megakadályozásához szükséges, akkor ideiglenes hozzáférhetetlenné tétel rendelhető el.

Ezt tehát a bíróság rendelheti el két módon: elektronikus adat ideiglenes eltávolításával, vagy elektronikus adathoz való hozzáférés ideiglenes megakadályozásával.

Az elektronikus adat ideiglenes hozzáférhetetlenné tételének teljesítésére kötelezett a bíróság megnevezésével és a határozat számának a megjelölésével tájékoztatja a felhasználókat a tartalom eltávolításának vagy a tartalomhoz hozzáférés megakadályozásának a jogalapjáról.

Az ideiglenes hozzáférhetetlenné tétel és az információs rendszerben tárolt adatok megőrzésére kötelezés együttesen is elrendelhető.

Az elektronikus adat ideiglenes eltávolítására az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló törvényben[49] meghatározott tárhelyszolgáltatót kell kötelezni. A kötelezett a határozat vele történő közlését követő egy munkanapon belül köteles az elektronikus adat ideiglenes eltávolítására.

Ebben az esetben tehát a vélhetően jogsértő adat magyar joghatóság alatt van, azaz a magyar bíróságok döntése kikényszeríthető magyar hatóságok által.

Az elektronikus adat ideiglenes hozzáférhetetlenné tételét a bíróság megszünteti, és az elektronikus adat visszaállítását rendeli el, ha az ideiglenes hozzáférhetetlenné tétel elrendelésének oka megszűnt, vagy a nyomozást megszüntették [kivéve, ha a Btk. 77. § (2) bekezdése alapján az elektronikus adat végleges hozzáférhetetlenné tétele elrendelésének lehet helye].

---

[46] Az intézkedés nem csak a büntetőeljárási törvényben, hanem az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. Törvény (Ektv) 12/A. §-ban is rögzítésre került 2012-ben.

[47] A nem közvádra üldözendők a magánvádas bűncselekmények (könnyű testi sértés, magántitok megsértése, levéltitok megsértése, rágalmazás, becsületsértés, kegyeletsértés)

[48] Az elektronikus adat végleges hozzáférhetetlenné tétele Btk. 77. §.

[49] Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény.

Az elektronikus adat ideiglenes hozzáférhetetlenné tétele a büntetőeljárás befejezésével megszűnik. Ha a bíróság az elektronikus adat végleges hozzáférhetetlenné tételét nem rendelte el, az elektronikus adat visszaállítására kötelezi a tárhelyszolgáltatót.

Az ideiglenes hozzáférhetetlenné tétel megszüntetéséről és az elektronikus adat visszaállításáról szóló határozatot a kötelezettel haladéktalanul közölni kell. A tárhelyszolgáltató a határozat vele történő közlésétől számított egy munkanapon belül köteles az elektronikus adat visszaállítására.

Az elektronikus adat ideiglenes eltávolítására és visszaállítására vonatkozó kötelezettség teljesítését a bírósági végrehajtó foganatosítja.

A bíróság hivatalból vagy az ügyész indítványára a tárhelyszolgáltatóval szemben az elektronikus adat ideiglenes eltávolítására vagy visszaállítására vonatkozó kötelezettség elmulasztása miatt százezer forinttól egymillió forintig terjedő rendbírságot szabhat ki, ami ismételten is kiszabható.

A másik fontos kapcsolódó jogintézmény az elektronikus adat ideiglenes hozzáférhetetlenné tétele, amelyre akkor van szükség, ha az elektronikus adat ideiglenes eltávolítása nem megvalósítható, mert az fizikálisan tipikusan nem magyar joghatóság alatt van. A Be. 158/D. § rendelkezései szerint a bíróság rendeli el, ha a tárhelyszolgáltató az elektronikus adat ideiglenes eltávolítására vonatkozó kötelezettséget nem teljesítette, vagy az elektronikus adat ideiglenes eltávolítására vonatkozóan a külföldi hatóság jogsegély iránti megkeresése a megkeresés kibocsátásától számított harminc napon belül nem vezetett eredményre, és a büntetőeljárás kábítószer-kereskedelem (Btk. 176–177. §), kóros szenvedélykeltés (Btk. 181. §), kábítószer készítésének elősegítése (Btk. 182. §), kábítószer-prekurzorral visszaélés (Btk. 183. §), új pszichoaktív anyaggal visszaélés (Btk. 184–184/A. §), gyermekpornográfia (Btk. 204. §), állam elleni bűncselekmény (Btk. XXIV. Fejezet), terrorcselekmény (Btk. 314–316. §) vagy terrorizmus finanszírozása (Btk. 318. §) miatt indult, és az elektronikus adat e bűncselekménnyel áll összefüggésben.

A bíróság a határozatával az elektronikus hírközlési szolgáltatókat kötelezi az elektronikus adathoz való hozzáférés ideiglenes megakadályozására.

Ha az elektronikus adat feletti rendelkezésre jogosult ismeretlen, az elektronikus adat ideiglenes hozzáférhetetlenné tételéről szóló határozatot hirdetményi úton kell kézbesíteni. A hirdetményt tizenöt napra ki kell függeszteni a bíróság hirdetőtáblájára, továbbá közzé kell tenni a bíróságok központi internetes honlapján.

A bíróság az elektronikus adat ideiglenes hozzáférhetetlenné tétele elrendeléséről elektronikus úton haladéktalanul értesíti az NMHH-t (Nemzeti Média- és Hírközlési Hatóság).

Az elektronikus adat ideiglenes hozzáférhetetlenné tételének a végrehajtását az NMHH szervezi és ellenőrzi. Az NMHH a bíróság elektronikus úton megküldött értesítése alapján az elektronikus adathoz való hozzáférés ideiglenes megakadályozására vonatkozó kötelezettséget bevezeti a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisába,[50] ezzel egyidejűleg a bíróság határozatáról elektronikus úton haladéktalanul értesíti az elektronikus hírközlési szolgáltatókat, amelyek az értesítéstől számított egy munkanapon belül kötelesek az elektronikus adathoz való hozzáférés ideiglenes megakadályozására. Ha valamely elektronikus hírközlési szolgáltató a kötelezettséget nem teljesíti, az NMHH erről haladéktalanul értesíti a bíróságot.

Az elektronikus adat ideiglenes hozzáférhetetlenné tételét a bíróság megszünteti, ha a tárhelyszolgáltató teljesíti az elektronikus adat ideiglenes eltávolítására vonatkozó kötelezettségét, az elrendelésének oka egyébként megszűnt, vagy a nyomozást megszüntették [kivéve, ha a Btk. 77. § (2) bekezdése alapján az elektronikus adat végleges hozzáférhetetlenné tétele elrendelésének lehet helye].

Az elektronikus adat ideiglenes hozzáférhetetlenné tételének megszüntetéséről a bíróság elektronikus úton haladéktalanul értesíti az NMHH-t, amely az elektronikus adathoz való hozzáférés ideiglenes megakadályozására vonatkozó kötelezettséget törli a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisából, és ezzel egyidejűleg a kötelezettség megszűnéséről elektronikus úton

[50] Bővebben: http://nmhh.hu/cikk/160577/Kozponti_elektronikus_hozzaferhetetlenne_teteli_hatarozatok_adatbazisa_KEHTA (a letöltés ideje: 2017. április 20.)

haladéktalanul értesíti az elektronikus hírközlési szolgáltatókat, amelyek az értesítéstől számított egy munkanapon belül kötelesek biztosítani az elektronikus adathoz a hozzáférést.

Az elektronikus adat ideiglenes hozzáférhetetlenné tétele a büntetőeljárás befejezésével megszűnik. Ha a bíróság az elektronikus adat végleges hozzáférhetetlenné tételét nem rendelte el, az ideiglenes hozzáférhetetlenné tétel megszűnéséről elektronikus úton haladéktalanul értesíti az NMHH-t, amely az elektronikus adathoz való hozzáférés ideiglenes megakadályozására vonatkozó kötelezettséget törli a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisából, és ezzel egyidejűleg a kötelezettség megszűnéséről elektronikus úton haladéktalanul értesíti az elektronikus hírközlési szolgáltatókat, amelyek az értesítéstől számított egy munkanapon belül kötelesek biztosítani az elektronikus adathoz a hozzáférést.

Ha valamely elektronikus hírközlési szolgáltató a hozzáférés újbóli biztosítására vonatkozó kötelezettséget nem teljesíti, az NMHH erről haladéktalanul értesíti a bíróságot.

A bíróság hivatalból vagy az ügyész indítványára az elektronikus hírközlési szolgáltatóval szemben az elektronikus adathoz való hozzáférés ideiglenes megakadályozására vagy a hozzáférés újbóli biztosítására vonatkozó kötelezettség elmulasztása miatt százezer forinttól egymillió forintig terjedő rendbírságot szabhat ki, ami ismételten is kiszabható.

A nyomozás során az elektronikus adat ideiglenes hozzáférhetetlenné tételének elrendelésére a nyomozó szerv vezetője teszi meg az előterjesztését az ügyészhez, aki ezt továbbítja a bírósághoz. Pozitív döntés esetén a bíróság a végrehajtón keresztül kötelezi a tárhelyszolgáltatót az ideiglenes eltávolításra.

Az esetek meglehetősen nagy számában a tárhelyszolgáltató nem rendelkezik magyarországi képviselettel, vagy sok esetben nem fellelhető, vagy honossága szerinti jogrendszerben a szólásszabadság megnyilvánulásának értelmezi azt, amit a magyar bíróság jogsértőnek talál.

Ha a bírósági döntés nem vezet eredményre, és a törvényben meghatározott súlyos bűncselekmények elkövetésének gyanúja áll fenn, a bíróság az NMHH-n keresztül tájékoztatja az elektronikus hírközlési szolgáltatókat, amelyek az értesítéstől számított egy munkanapon belül kötelesek az elektronikus adathoz való hozzáférés ideiglenes megakadályozására, azaz például a külföldi szervereken a vélelmezhetően jogsértő tartalom elérhető, de azt a magyar szolgáltatók szűrik és elérhetetlenné teszik.[51]

E jogintézményhez hasonló az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (Ektv) 13. §-ban rögzített „Értesítés a jogsértő információs társadalommal összefüggő szolgáltatásról" jogintézményéhez. A jogalkotó ebben az esetben a jogsértő tartalmak eltávolítására kötelezés kezdeményezését a jogaiban sértett személy közvetlen lehetőségévé teszi az információs társadalommal összefüggő szolgáltatást nyújtó természetes, illetve jogi személy vagy jogi személyiség nélküli szervezet irányába.

Itt viszont a sérelem a szellemi tulajdonában sértett jogokra, illetve kiskorú személy személyiségi jogaira vonatkozik, és nem szükséges hozzá bűncselekmény megvalósulásának gyanúja.

8.1.7.6. Kapcsolódó büntető törvénykönyvi rendelkezések

Amíg a büntető eljárásjogi törvény a formáját adja meg a bűncselekmények elkövetőinek felelősségre vonásának, addig a büntető törvénykönyv meghatározza, mely jogsértő cselekmények tekintendők bűncselekményeknek, és meghatározza, hogy azokhoz milyen büntetési formából, típusból milyen mértéket szabhatnak ki a bíróságok.

[51] Ez a rendszer sokban hasonlít a NAV által betiltott szerencsejáték oldalakra, de ott a jogalapot a szerencsejáték szervezéséről szóló 1991. évi XXXIV. törvény 36/H. § adja és nem a büntetőeljárás. Bővebben: www.nav.gov.hu/nav/szerencsejatek/blokkolt_honlapok (a letöltés ideje: 2017. április 20.)

8.1.7.7. Az elektronikus adat végleges hozzáférhetetlenné tétele

Ezen alfejezetben tehát már nem egy büntetőeljárási cselekmény részletszabályaival foglalkozunk, hanem a büntetőeljárás egyik lehetséges végső eredményével.

A végleges hozzáférhetetlenné tételt a büntető törvénykönyvről szóló 2012. évi C. törvény 77. §-a szabályozza az intézkedések fejezetben, többek között a megrovás, a próbára bocsátás, a jóvátételi munka, az elkobzás, a vagyonelkobzás és további intézkedési formák mellett.[52]

Btk. 77. § (1) bekezdése szerint véglegesen hozzáférhetetlenné kell tenni azt az elektronikus hírközlő hálózaton közzétett adatot, amelynek hozzáférhetővé tétele vagy közzététele bűncselekményt valósít meg, amelyet a bűncselekmény elkövetéséhez eszközül használtak, vagy amely bűncselekmény elkövetése útján jött létre. A (2) bekezdés értelmében az elektronikus adat végleges hozzáférhetetlenné tételét akkor is el kell rendelni, ha az elkövető gyermekkor, kóros elmeállapot, vagy törvényben meghatározott büntethetőséget megszüntető ok miatt nem büntethető, illetve, ha az elkövetőt megrovásban részesítették.

Végrehajtásáról a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról szóló 2013. évi CCXL. törvény 324. §-a és a Be. 596/A. §-a rendelkezik.

Az intézkedés teljesítésére az elektronikus kereskedelmi szolgáltatások, valamint a tárhelyszolgáltató köteles egy munkanapon belül, és a bírósági végrehajtó hajtja végre. Esetleges elmulasztása miatt a büntetés-végrehajtási bíró a tárhelyszolgáltatóval szemben százezer forinttól egymillió forintig terjedő pénzbírságot szabhat ki. A pénzbírság háromhavonta ismételten kiszabható.

Külföldi szolgáltató nem teljesítése esetén igazságügyi végrehajtási jogsegély kezdeményezhető, amely meglehetősen hosszú időt vesz igénybe, és nem biztosított a végrehajtása sem.

8.1.8. Nemzetközi rendészeti együttműködés a kiberbűnözés területén

A nemzetközi rendészeti együttműködés fontossága a kiberbűncselekmények területén megkérdőjelezhetetlen. A lisszaboni szerződés jelentősen leegyszerűsítette az intézményi keretet (EUMSZ), így a rendőri együttműködésre vonatkozó intézkedések nagy része jelenleg a rendes jogalkotási eljárás (együttdöntési eljárás) keretében kerül elfogadásra, felülvizsgálatuk pedig a bíróság hatáskörébe tartozik. Mindazonáltal, még ha el is tekintünk a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség sajátosságaitól (az Egyesült Királyságra, Írországra és Dániára vonatkozó mentességek, a nemzeti parlamentek kiváltságos szerepe), a rendőrségi együttműködés és a büntetőügyekben folytatott igazságügyi együttműködés nem vált maradéktalanul a közösségi keret részévé, és részben továbbra is megőrzi eredeti sajátosságait:

- a Bizottság megosztja a tagállamokkal a kezdeményezési jogkörét, ha utóbbiak a Tanács tagjainak egynegyedét képviselik (az EUMSZ 76. cikke);
- az Európai Parlamenttel csupán konzultálnak az operatív együttműködési intézkedésekről, melyeket a Tanács egyhangúlag fogad el. Amennyiben a Tanácsban nincs egyhangúság, kilenc vagy több tagállam megerősített együttműködése alapján működhet. Ebben az esetben az Európai Tanács felfüggeszti a folyamatot, hogy konszenzust keressen [az úgynevezett „felfüggesztő eljárás", az EUMSZ 87. cikkének (3) bekezdése];
- az EUMSZ hatálybalépése előtt elfogadott jogi aktusok 5 éven belül nem képezhetik kötelezettségszegési eljárás tárgyát, illetve azokra vonatkozóan nem nyújtható be a Bírósághoz előzetes döntéshozatal iránti kérelem (az EUMSZ-hez csatolt 36. jegyzőkönyv). Ez az időszak 2014 decemberében ért véget.

[52] A büntető törvénykönyv értelmében a bíróság szankcióként büntetéseket (szabadságvesztés, pénzbüntetés, közügyektől eltiltás stb.) valamint intézkedéseket alkalmazhat.

8.1.8.1. Az Egyesült Nemzetek Szervezete (ENSZ)

Az Egyesült Nemzetek Szervezete részéről több dokumentum foglalkozik az informatikai bűncselekmények megelőzésével, kezelésével, az információs technológiák elleni harccal.[53] Az 1994-ben kiadott kézikönyv − a számítógépes bűncselekmények megelőzéséről és kezeléséről − a *számítógépes bűncselekmény* (computer crime), valamint a *számítógéppel kapcsolatos bűncselekmény* (computer-related crime) fogalmakat még nem határolja el. Felsorolja ugyanakkor a leggyakoribb számítógépes bűncselekménytípusokat, mint a számítógép manipulációjával elkövetett csalás, a számítógépes hamisítás, a károkozás számítógépes adatokban vagy programokban, illetve a számítógépes adatok vagy programok megváltoztatása, a jogosulatlan hozzáférés számítógépes rendszerekhez és szolgáltatásokhoz, a jogi védelem alá eső számítógépes programok jogosulatlan reprodukálása. A kézikönyv támaszkodik az *ET ajánlásra*.[54] Felismerték, hogy a számítógépes környezetben elkövetett bűncselekményekkel szemben nem elegendő a területi védekezés, mivel az a deliktum jellege miatt egy kiterjedtebb kört veszélyeztet.

Ugyanakkor a gyermekpornográfia bűncselekménye vagy épp a cyberbullying (vagy más néven elektronikus zaklatás) miatt, kiemelést érdemel az 1989-es gyermekek jogairól szóló New York-i egyezmény, mely több szabályt is tartalmazott a gyermek káros tartalmakkal szembeni védelméről.

Az ENSZ közgyűlése a 2000-ben elfogadott határozatában már az információs technológiák bűncselekményekhez való felhasználásával szembeni harcra hívja fel a figyelmet, és olyan intézkedéseket azonosított, amelyek segítenek az információs technológiákkal való visszaélés megelőzésében, illetve az ezek elleni fellépésben. Így például az államok jogszabályai és joggyakorlata számolja fel a védett zónákat az információs technológiákkal való visszaélések esetében, mikor is koordinálni kell az érintett államok között a nyomozó hatóságok együttműködését a nyomozásban és a vádemelésben. Legyen biztosított az információmegosztás az államok között, valamint a nyomozó hatóságok személyzetének kiképezése és felszereléssel ellátása. A jogrendszereknek védeniük kell az adatok számítógépes bizalmasságát, integritását és elérhetőségét a jogosulatlan megkárosítástól, és biztosítaniuk kell, hogy a visszaéléseket büntetni rendelik. A jogrendszereknek lehetővé kell tenniük a bűnügyi nyomozásokkal kapcsolatos elektronikus adatok megőrzését, és az ezekhez való gyors hozzáférést. A határozat rámutat, hogy a nyilvánosság figyelmének felhívása a személyes szabadságjogok és a magánélet védelmének, valamint a kormányzat cselekvési lehetőségeinek megőrzésére, az ilyen jellegű visszaélések elleni küzdelem része.

8.1.8.2. Gazdasági Együttműködési és Fejlesztési Szervezet (OECD):

A Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) az, amely vizsgálta a számítógépes bűncselekményekkel kapcsolatos európai helyzetet, és összegezte a tapasztalatokat. Az általuk elvégzett vizsgálatokkal és a megállapításaikkal egy olyan iránymutatást akartak írni, amely felhasználható az informatikai bűncselekmények jellemzőinek megismeréséhez.

Az OECD a következőképpen rendszerezi a tapasztalatokat a számítógépes bűncselekményekkel kapcsolatban:

- számítógépes adatok és/vagy programok bevitele, módosítása, törlése vagy
- elmentése jogtalan vagyoni eszközök vagy más értékek megszerzése céljából;
- számítógépes adatok és/vagy programok bevitele, módosítása, törlése vagy
- elmentése hamisítás céljából;
- számítógépes adatok és/vagy programok bevitele, módosítása, törlése vagy

[53] Az ENSZ Kézikönyve a számítógéppel kapcsolatos bűncselekmények megelőzéséről és kezeléséről (1994); Az ENSZ Közgyűlésének 55/63 számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról; Az ENSZ Közgyűlésének 56/121 számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról.

[54] UN Manual on the Prevention and Control of Computer-Related Crime vagyis a Számítógépes Bűnözés megelőzéséről és szabályozásáról szóló tanulmány.

- elmentése, vagy a számítógépbe történő bármely más beavatkozás a számítógépes vagy telekommunikációs rendszerek funkcióinak megakadályozása céljából;
- a védett számítógépes programok tulajdonosai exkluzív jogainak megsértése a program jogosulatlan hasznosítása vagy forgalomba hozatala révén;
- a számítógépes vagy telekommunikációs rendszerbe az arra jogosult engedélye nélkül, vagy a biztonsági intézkedések megsértésével, vagy más tisztességtelen, netán bűnös szándékkal történő belépés, vagy annak lehallgatása.

8.1.8.3. Az Európa Tanács (ET)

Az ET 2001. november 23-án Budapesten fogadta el a Számítástechnikai bűnözésről szóló egyezményt (Convention of Cybercrime), ami 2004. július 1-jén lépett hatályba. Az Európa Tanács 5 tagállama – így Magyarország[55] is – ratifikálta a konvenciót. 2011. október 1-ig az Európa Tanács 31 tagja, valamint az Egyesült Államok részéről is megtörtént az egyezmény elfogadása és törvénybe iktatása. A számítástechnikai bűnözésről szóló egyezményt a számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szóló kiegészítő jegyzőkönyv[56] követte.

A számítástechnikai bűnözésről szóló egyezmény védeni kívánja a számítástechnikai rendszerek, a hálózatok, az adatok hozzáférhetőségének sérthetetlenségét, az ilyen rendszerek titkosságát. Biztosítani kívánja a rendszerek, a hálózatok, az adatok visszaélésszerű használatának megelőzését és bűncselekménnyé nyilvánítását is. Továbbá meghatározza a számítógépes bűnözés elleni hatékony fellépést lehetővé tévő felderítést, a nyomozást és bűnüldözést, nemzeti és nemzetközi szinten. Az értelmező rendelkezések körében az egyezmény több alapfogalmat definiál: *számítástechnikai rendszer* (computer system), *számítástechnikai adat* (computer data), *szolgáltató* (service provider), illetve *forgalmi adat* (traffic data), ugyanakkor a *számítástechnikai bűncselekmény* (cybercrime) fogalmának meghatározásával adós marad. Az egyezmény a büntető anyagi jogi szabályok körében négy csoportra osztja a bűncselekményeket. Az elsőt a számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények adják, a második csoportot a számítógéppel kapcsolatos bűncselekmények, a harmadikat a számítástechnikai adatok tartalmával kapcsolatos bűncselekmények, a negyedik csoportot pedig a szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények.

Uniós jogi aktusok az informatikai bűncselekményekkel kapcsolatosan

- Az Európai Parlament és a Tanács 2000/31/EK irányelve a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem egyes jogi vonatkozásairól („Elektronikus kereskedelemről szóló irányelv” – 2000);
- A Tanács 2001/413/IB számú kerethatározata a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről (2001);
- A Tanács 2005/222/IB kerethatározata az információs rendszerek elleni támadásokról (2005);
- Az Európai Parlament és a Tanács 2006/24/EK irányelve a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról (2006); *(Megjegyzendő: az adatmegőrzési irányelvet az Európai Unió Bírósága*

[55] A 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről.

[56] A számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szóló kiegészítő jegyzőkönyv -

2014. április 8. napján az Európai Unió Alapjogi Chartájával való ütközése miatt érvénytelennek nyilvánította)
– Az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról.

8.1.8.4. Az Európai Tanács

Az Európai Tanács megbízásából 1994-ben a következő, az információs társadalommal szemben tanúsított alábbi elvárásokat (célkitűzéseket) fogalmazták meg:
- Az informatikai eszközöket szabványosítani kell.
- Ha nem szabványosak az eszközök, elveszik a lényeg, az információáramlás.
- Azért kell szabványosítani, mert az üzleti élet, a versenyszféra ellenérdekelt.
- A monopolhelyzeteket meg kell szüntetni, különösen a telekommunikációval kapcsolatban. (A jog hosszú ideig elfogadta a monopolhelyzetet, mert a beruházás e területeken nagyon sokba kerül, de most már nem fogadják el ezt az érvelést.)
- Biztosítani kell a szellemi alkotások megfelelő szintű védelmét. A szerzői jogban teljesen új terület a zene-, kép-, filmletöltések, melyekre még akkor sem volt és ma nincs megfelelő szabályozás, védelem.
- Kiemelt fontosságú a magánszféra védelme, mivel ez van kitéve a legnagyobb veszélynek. Felismerték, hogy a mai világban a magánszférát egyetlen eszközzel lehet védeni, és ez a jog. A magánszemélyt technikai eszközzel már nem lehet az állammal szemben megvédeni.
- Elvárt az adatbiztonság szabályainak kidolgozása (vírusok elleni védelem; olyan rendszert nem lehet építeni, amibe nem lehet belenyúlni, de olyat igen, amelyben az illetéktelen belépés nem marad észrevétlen).

Az Európai Unió Tanácsa 2005 februárjában elfogadta az információs rendszerek elleni támadásról szóló 2005/222/IB kerethatározatot, amelyben a korábban használatos *számítógépes rendszer* fogalom helyett már az *információs rendszer* (information system) jelenik meg. Az egyes fogalmak összevetésekor megfigyelhető, hogy annak ellenére, hogy a megjelölés különbözik, a fogalmak tartalma gyakorlatilag megegyező. A kerethatározat az üldözendő magatartásokat a következőkben csoportosítja:
1. információs rendszerekhez való jogsértő hozzáférés;
2. rendszerbe való jogsértő beavatkozás;
3. adatokba való jogsértő beavatkozás.

A kerethatározatot 2013-ban felváltotta az információs rendszerek elleni támadásokról szóló 2013/40/EU irányelv. Az új irányelv különös figyelmet fordít az úgynevezett botnetekre és a személyazonossághoz kapcsolódó bűncselekményekre, valamint súlyosabb szankciókat helyez kilátásba abban az esetben, ha az informatikai bűncselekményt bűnszervezetben követik el. Ezenfelül előírja, hogy a büntetőeljárás során figyelembe kell venni azt a körülményt, ha a bűncselekményt az elkövető alkalmazotti minőségben követi el.

8.1.8.5. Az Európai Unió Belső Biztonsági Állandó Bizottsága (COSI)

Az Európai Unió Belső Biztonsági Állandó Bizottsága (COSI) meghatározta a stratégiai célokat a számítógépes bűnözés területén. Az Állandó Bizottság célja a belső biztonság területén, hogy megkönnyítse a tagállamok közötti operatív tevékenységek koordinálását. A belső biztonsággal kapcsolatban ez az operatív együttműködéssel kapcsolatos rendőrségi és vámügyi együttműködést, a külső határok

védelmét és a büntetőügyekben folytatott igazságügyi együttműködést érinti. A COSI operatív szerepére tekintettel Magyarországot a Belügyminisztérium képviseli.

A 2014–2017 közötti időszakban a COSI elsősorban

- a nagy károkozással járó, online és bankkártyás fizetéssel összefüggő, továbbá
- az áldozatok részére komoly hátránnyal járó – például gyermekek sérelmére elkövetett – számítógépes bűncselekmények, valamint
- a kritikus infrastruktúrát és számítógépes rendszereket érintő informatikai bűncselekmények tekintetében kíván hatékony lépéseket tenni a kialakítandó védekezés érdekében.

A stratégia kitér a lehetséges informatikai rendszersebezhetőségek beazonosításának problematikájára is. Az informatikai támadásokat okozó bűnözést illetően is definiálták a problémákat, melyek a következők:

- kevés információ a bűnözői hálózatokról;
- a kockázatokhoz kapcsolódó tudatosság hiánya;
- jogi akadályok fennállta az információcserében;
- az elégtelen bűnfelderítői együttműködés;
- az állam jogalkalmazó és igazságszolgáltató szerveinek elégtelen felkészültsége;
- az incidensek azonosításának és besorolásának országonként eltérő formája;
- a civilszféra alacsony szintű bevonása;
- az Európai Unión kívüli cselekmények jelentős hatása;
- az alacsony mértékű felderítés;
- alacsony szám a bűnelkövetői elfogások terén.[57]

8.1.8.6. Az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA)

Az Európai Parlament és a Tanács 460/2004/EK rendelete szól az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) létrehozásáról, amely egy kiberbiztonsági szakértői központként működik Európában.

Az EU azért tartotta szükségesnek a létrehozását, mert az informatikai támadások veszélyeztetik a tagállamok állampolgárainak biztonságát, és a számítógépes rendszerek elleni bűncselekmények jelentős anyagi kárt okoznak a nemzetgazdaságnak. Az ENISA független szerv.

Az ügynökség székhelye Görögországban, Heraklionban (Kréta) található, az operatív iroda pedig Athénban.

Az ügynökség célkitűzései között szerepel, hogy „az EU-tagállamok és az üzleti szféra fokozottabb mértékben legyen képes a hálózat- és információbiztonsággal kapcsolatos problémák megelőzésére, kezelésére és az azokra történő reagálásra."[58] További feladat a segítségnyújtás, a tanácsadás jogi és technikai kérdésekben a tagállamok és az Európai Bizottság számára.

Az ügynökség szorosan együttműködik a tagállamokkal és a magánszektorral, úgy, hogy tanácsot és megoldásokat kínál nekik. Ez az együttműködés magában foglalja, a páneurópai kiberbiztonsági gyakorlatokat, a National Cyber Security stratégiák fejlesztését, CSIRT-ek együttműködésének elősegítését, a kapacitásbővítést, az adatvédelmi kérdések kezelését, az adatvédelmet erősítő technológiák és a magánéletben megjelenő új technológiák erősítését.

Feladatai:

- összegyűjti az információkat kockázatok elemzéséhez, amiről tájékoztatja az EU-tagállamokat és a Bizottságot;

[57] www.cert-hungary.hu/node/212 (a letöltés ideje: 2014. szeptember 26.)

[58] http://europa.eu/legislation_summaries/information_society/internet/l24153_hu.htm (a letöltés ideje: 2014.szeptember 26.)

- az Európai Parlament, a Bizottság, az illetékes európai és nemzeti szervek számára tanácsot, illetve adott esetben segítséget nyújt;
- fokozza az együttműködést;
- elősegíti a Bizottság és a tagállamok közötti együttműködést a biztonsági problémák megelőzésére szolgáló közös módszerek kidolgozásában;
- hozzájárul a tudatosság növeléséhez és ahhoz, hogy a hálózat- és információbiztonsággal kapcsolatos kérdésekre vonatkozóan naprakész, tárgyilagos és átfogó információk legyenek elérhetők valamennyi felhasználó számára;
- segíti a Bizottságot és a tagállamokat az iparral folytatott hardver- és szoftvertermékek biztonságával kapcsolatos problémákról szóló párbeszédben;
- nyomon követi a biztonsági termékek és szolgáltatások szabványainak kialakítását, valamint előmozdítja a kockázatértékelési és kockázatkezelési tevékenységeket;
- hozzájárul az EU-n kívüli országokkal és nemzetközi szervezetekkel folytatott együttműködést célzó, uniós szintű erőfeszítésekhez, hogy elősegítse a biztonsági kérdésekre vonatkozó globális szemlélet terjedését;
- megfogalmazza saját következtetéseit, iránymutatásait, valamint tanácsot ad.[59]

Az ENISA három tevékenységi területen aktív: ajánlásokat készít, olyan tevékenységeket végez, amelyek segítik a politikai döntéshozatalt és végrehajtást, s jellemző rá a „Hands On” munka, amikor az ENISA együttműködik közvetlenül a műveleti csoportokkal EU-szerte.

8.1.8.7. Az Europol

Az Europol az Európai Unió bűnüldöző hatósága, amelynek fő feladata, hogy tevékenységével segítse az unió biztonságosabbá tételét. Ez az Európai Unió kormányközi, koordinációs és jogi végrehajtó szervezete. Feladatai közé tartozik az EU-tagállamok hatóságainak támogatása, a kölcsönös információmegosztás a nemzeti rendőrségekkel, és a különböző bűnügyi adatok szakszerű elemzése. Hatáskörébe tartozik többek között a terrorizmus, a kábítószer-kereskedelem, a nemzetközi szervezett bűnözés, az ipari jog megsértése és a termékhamisítás, az illegális bevándorlás, továbbá a lopott autók csempészése, a pénzmosás és az euró hamisítása elleni fellépés és megelőzés.

Hivatalos ügynökséggé 2010-ben vált, ezáltal egy sokkal integráltabb együttműködés kialakítása, kidolgozása lett a fő feladata. Az Europol célja, hogy javítsa az európai bűnüldöző hatóságok eredményességét és együttműködését a nemzetközi bűnözés súlyos formái, a szervezett bűnözés és a terrorizmus megelőzésében és leküzdésében. Az Europol szorosan együttműködve végzi a tevékenységét az Európai Unió 27 tagállamának bűnügyi hatóságaival, csakúgy, mint az USA, Kanada, Ausztrália és Norvégia bűnüldöző szerveivel. Ennek eredményeképp az Europol évi 13 500, határokon átnyúló nyomozáshoz nyújt hathatós segítséget, elsősorban az adatbegyűjtés, - elemzés, és -megosztás, valamint a koordináció eszközeivel. Az Europol eseti alapon részt vesz még a tagállamok területén tevékenykedő, úgynevezett Közös Nyomozó Csoportok munkájában, ahol speciális eszközökkel és információkkal segíti a bűntények felderítését. Az Europol munkáját ezen felül segíti még a tagállamok és partnerországok által delegált, mintegy 145 összekötő tiszt is, akik az Europol székházában, Hágában tartanak fenn irodát, és a minél gyorsabb és hatékonyabb együttműködést, a személyes kapcsolatokat és a kölcsönös bizalom kiépítését segítik elő.

[59] http://europa.eu/legislation_summaries/information_society/internet/l24153_hu.htm (a letöltés ideje: 2017. április 20.)

Az Europol tevékenysége[60]

Az Europol 1999. július 1-jén kezdte meg teljes körű működését, azt követően, hogy a tagállamok ratifikálták az Europol-egyezményt. 2010. január 1-jén az ezen egyezmény helyébe lépő, az Európai Rendőrségi Hivatal (Europol) létrehozásáról szóló 2009. április 6.-i, 2009/371/IB számú tanácsi határozat (tanácsi határozat) elfogadása után, az Europol új jogi kerettel és kiterjesztett feladatkörrel rendelkező, teljes jogú uniós ügynökséggé vált.

Az Europol tagállamoknak nyújtott támogatása a következőket foglalja magában:

- az információcsere és a bűnügyi hírszerzés megkönnyítése az európai bűnüldöző hatóságok között az Europol információs és elemző rendszerei, valamint a biztonságos információcsere-hálózati alkalmazás (SIENA) segítségével;
- a tagállamok műveleteihez műveleti elemzés készítése, illetve támogatás nyújtása;
- a tagállamoktól vagy egyéb forrásból, illetve az Europoltól származó információk és adatok alapján stratégiai jelentések (például veszélyértékelések) és bűnügyi elemzések készítése;
- szakértelem és technikai támogatás biztosítása az EU-n belüli nyomozásokhoz és műveletekhez, az érintett tagállamok felügyelete és jogi felelőssége mellett.

Az Europol a fentieken kívül a bűnügyi elemzések elősegítésével, a nyomozási technikák harmonizálásával és a tagállamokban adott képzésekkel is foglalkozik.

Ezen feladatai ellátásában segíti az Europol Információs Rendszer (továbbiakban: IS), amely lényegét tekintve az Europol bűnügyi adatbázisa, elsődleges ellenőrző rendszere. Működtetésének célja, hogy az Europol mandátumába tartozó, súlyos megítélésű (a Btk. szerint legalább 5 év szabadságvesztéssel fenyegetett), és legalább két tagországot érintő bűncselekmények esetén a tagállamokban folyamatban levő nyomozásokat összekapcsolja, ezáltal orientálva és támogatva a nemzeti bűnüldöző hatóságok operatív, műveleti tevékenységét. Az IS gyakorlati haszna abban áll, hogy segítségével megállapítható, hogy az Europol mandátumába tartozó ügyek esetében egy másik Europol-tagország rendelkezik-e a hazai nyomozáshoz kapcsolható információval. „Találat" esetén a tagállamok adatszolgáltató nyomozó szervei a nemzeti egységek közvetítése révén kapcsolatba léphetnek egymással, és megállapodhatnak az információk felhasználhatóságát illetően. Magyarországon az Europol Nemzeti Egység az Országos Rendőr-főkapitányság Nemzetközi Bűnügyi Együttműködési Központjában (ORFK NEBEK Iroda) található.

Az Europol ellenőrzése, az adatvédelem

Az Europol a magánszemélyekre vonatkozóan jelentős mennyiségű érzékeny adatot kezel, és fontos, hogy ezek felhasználása során tekintettel legyen a személyiségi jogokra. Ennek ellenőrzését egy úgynevezett Közös Ellenőrző Hatóság végzi. Az Europolt és a Közös Ellenőrző Hatóságot is létrehozó, az Európai Rendőrségi Hivatal (Europol) létrehozásáról szóló 2009. április 6.-i, 2009/371/IB számú tanácsi határozat (tanácsi határozat) védintézkedésként számos adatvédelmi rendelkezést tartalmaz. A Közös Ellenőrző Hatóság – mint független szerv – a tagállamok adatvédelmi hatóságai által delegált tagokból áll, és legfontosabb feladata annak biztosítása, hogy az Europol megfeleljen az adatvédelmi elveknek. Magyarországon a nemzeti adatvédelmi hatóság feladatait 2012. január 1. óta a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) látja el.

Ellenőrzési tevékenysége során a Közös Ellenőrző Hatóság rendszeresen felülvizsgálja az Europol tevékenységét, annak biztosítása érdekében, hogy az Europol birtokában lévő adatok tárolása, feldolgozása és felhasználása ne sértse a személyiségi jogokat. Ezt az általános feladatot a Közös Ellenőrző Hatóság részben úgy teljesíti, hogy vizsgálatokat végez az Europollal kapcsolatban. A Közös

[60] http://europol.europa.eu (a letöltés idehje: 2017. április 20.)

Ellenőrző Hatóság annak mérlegeléséért is felelős, hogy az Europol betartja-e az adatvédelmi elveket számos konkrét területen. E konkrét feladatok között szerepel konkrét elemzési munkafájlok létrehozásának vizsgálata és véleményezése; az Europoltól származó adatok továbbítása, engedélyezhetőségének nyomon követése; az Europol személyes adatfeldolgozásra és -felhasználásra vonatkozó tevékenységeivel összefüggő végrehajtási és értelmezési kérdések vizsgálata; a személyes adatoknak az Europol általi – uniós intézmények, szervek, hivatalok és ügynökségek, harmadik szervek és nem tagállamok részére történő – továbbításának nyomon követése, továbbá létező problémákra vonatkozó közös megoldásokra irányuló, egyeztetett javaslatok kidolgozása. A Közös Ellenőrző Hatóság felelős azért is, hogy támogassa a magánszemélyeknek a személyes adataikhoz fűződő jogainak érvényesítését. Idetartozik azon magánszemélyek fellebbezésének elbírálása is, akik tájékoztatást kértek a velük kapcsolatos adatokról, de elégedetlenek az Europol válaszával.

Az EUROPOL felállított egy Csúcstechnológiai Bűnözés Elleni Központot, amely 3 területen tevékenykedik munkacsoportokban: a gyermekek szexuális kizsákmányolása; bankkártyacsalások és a 3. munkacsoport, amelyből 2013. januárjában megalakult az EC3.

A Számítástechnikai bűnözés Elleni Központ (European Cybercrime Centre, EC3)

Az Európai Bizottság 2012. március 28-án nyújtotta be javaslatát a számítástechnikai bűnözés elleni küzdelem európai központjának létrehozására. A központot Hágában az Európai Rendőrségi Hivatalon belül hozták létre, és működését 2013.január 11-én kezdte meg. Célja, hogy:

- európai kapcsolattartó pontként működjön a számítástechnikai bűnözés elleni küzdelemben;
- részt vegyen az unión belüli rendészeti koordinációban;
- operatív támogatással segítse a tagállami rendészeti szerveket a konkrét nyomozások során;
- a Központ feladata elsősorban a kiberbűnözés elleni harc koordinálása, különös hangsúlyt fektetve a nagy nyereséggel járó bűnözés elleni tevékenységre;
- a személyazonosság-lopás elleni küzdelem;
- az elektronikus bankszolgáltatásokat érintő bűncselekmények elleni harc;
- a gyermekek szexuális kizsákmányolása elleni harc;
- az Európai Unió kritikus infrastruktúráinak és informatikai rendszereinek korlátozott védelme.

Az EC3 45 főből áll, többek között elsőrendű kibernetikai szakértőkkel kezdte meg tevékenységét. Nincs önálló nyomozati jogköre. Adatgyűjtést végez egy kiberbűnözési helpdesk üzemeltetésével a tagállami nyomozóhatóságok részére, vagyis támogatja tagállamok kiberbűnözések elleni nyomozásait azzal, hogy segíti a közös nyomozócsoportok létrehozását egy vagy több tagállam együttműködésével, valamint megteremti és koordinálja a tagállamok közötti együttműködést. Továbbá szoros együttműködést teremt az EUROJUST-tal és az INTERPOL-lal (e két szervezeteről bővebben lásd lentebb). Az EC3 értékeli és elemzi a kibertérből érkező fenyegetéseket, módszereket, ezekből előrejelzi a kiberbűnözés alakulását. Fontos a magánszektorral történő szoros együttműködés, valamint a CERT-ekkel történő kapcsolattartás, annak érdekében, hogy felkészültek legyenek a kibertámadásokkal kapcsolatban, és fel tudjanak lépni ellene. Kutatás és fejlesztés (K+F) és a képzés során szorosan együttműködik a CEPOL-lal, a tagállamok nyomozó hatóságaival és igazságügyi szervezeteivel, akiknek a folyamatos képzését, forenzikus eszközeik fejlesztését támogatja. Az EC3 hatáskörébe tartozó fókuszpontok a számítógépek és a hálózati infrastruktúrák ellen végrehajtott bűncselekmény kivizsgálása, valamint a különböző internetes bűncselekmények (FP Cyborg), a gyermekek szexuális kizsákmányolása (FP Twins) mellett a bankkártyákkal történő csalások és a személyes adatokkal történő visszaélések is (FP Terminal).

A központ kiemelt feladata, hogy figyelmeztesse a tagállamokat az esetleges fenyegetésekre. Szintén lényeges lépés az online szervezett bűnözői csoportok felkutatásának és azonosításának támogatása, ezt erősítve a központ tagállami szinten is képes segítséget nyújtani konkrét nyomozásokhoz.

8.1.8.8. A Kooperatív Kibervédelmi Kiválósági Központ (Cooperative Cyber Defence Centre of Excellence – CCD COE)

Központja Tallinban, Észtországban van. A szervezet egyidejűleg működik a NATO további 15 kiválósági központjával, melyek a Szövetséges Transzformációs Parancsnokságnak (Allied Command Transformation – ACT) alárendelve dolgoznak, azonos céllal: az adott terület szakértőinek támogatása és a Szövetség tagállamainak az adott kérdéssel kapcsolatos képességeinek fejlesztése.

A Központ több ország kooperációjával jött létre: Észtország, Németország, Olaszország, Litvánia, Lettország, Szlovákia, Spanyolország voltak az alapító tagok. Magyarország 2010-ben csatlakozott a Központhoz, az Amerikai Egyesült Államok megfigyelő státuszban van jelen, Törökország pedig mint támogató állam már 2008-ban bejelentette igényét a Központhoz való csatlakozásra.[61]

A központ feladatai közé tartozik többek között:

- a tagállamok kiberképességeinek fejlesztésének támogatása;
- a tagállami doktrínák, koncepciók és stratégiák kidolgozásának támogatása;
- az információs biztonság oktatása, képzések és gyakorlatok lebonyolítása;
- a kibernetikai védelem és a kiberhadviselés jogi vonatkozásainak elemzése, lépések megtétele a nemzetközi jogi keretek megalkotására.

8.1.8.9. Cyber Defence Management Authority – CDMA

A Központ mellett a NATO létrehozta a kibervédelmi problémákkal foglalkozó hatóságot (Cyber Defence Management Authority – CDMA) is, ami egy igazgatóság (Cyber Defence Management Board – CDMB) alá rendelve végzi el feladatait. Ennek székhelye Brüsszel, és feladata a szövetségi szintű centralizált kibervédelem irányításának megteremtése. A NATO-t és a tagállamokat érő támadásokra való reagálás, valamint a tagállami szintű segítésnyújtás a nemzeti kibervédelem kialakításában is segítséget nyújt, amelyben gyorsreagálású csapatokat (Rapid-Reaction Teams) hoztak létre, hogy ezek nemzeti szinten nyújtsanak segítséget a támadások ellen.

8.1.8.10. Computer Emergency Response Teamek (CERT)

A nemzeti szinten létrehozott CERT egy szakértőkből álló „testület”, amely a nemzeti hálózatok felügyeletét és adott esetben annak védelmének kidolgozását végzi. Ma több mint 250 ilyen CERT létezik – többek között Magyarországon is –, és bevett gyakorlattá vált, hogy az államok pénzügyi támogatásával ezek a csoportok látják el a nemzeti kibervédelmi felügyeletet. A bukaresti csúcs után a védelmi miniszterek támogatták azt az ötletet, hogy minden tagállam alapítsa meg a saját reagáló csapatát, ezzel is erősítve a CDMA munkáját.

8.1.8.11. International Telecommunications Union (ITU)

Az informatikai bűncselekmények elleni nemzetközi fellépés szükségessége, az internacionális együttműködés hatékonysága nem lehet kétséges a deliktumok országok határait átlépő jellege miatt. A digitális világ védelmében és biztonságának megőrzésében, azaz összefoglaló néven a kiberbiztonság eszközeinek tekinthető intézkedések megtételéhez relatíve egységes fogalmak szükségesek. A *kiberbiztonság* jogi, technikai és szervezeti kihívásokat jelent, és mivel ezek globális jellegűek, szükségessé

[61] www.biztonsagpolitika.hu/?id=16&aid=1125&title=A_NATO_kiberv%C3%A9delmi_politik%C3%A1j%C3%A1nak_%C3%A1ttekint%C3%A9se (a letöltés ideje: 2014. szeptember 27.)

vált egy koherens, nemzetközi együttműködés keretein belüli stratégiának a kialakítása. Csak egy ilyen jellegű stratégia alkalmas az érintett országok szerepének meghatározására, illetve a már létező stratégiák számbavételére. A nemzetközi együttműködés szükségességét felismerve több internacionális szervezet foglalkozik a kiberbiztonság kérdésével. Ezek közül is kiemelkedik az ITU, az általa megalkotott Global Cybercrime Agenda, valamint az Európai Unió Kiberberbiztonsági Stratégiája.

Az ITU X.1205 számú ajánlása a *kiberbiztonság* fogalmát – a lényegi elemek meghatározásával – a következők szerint definiálja:

„A kiberbiztonság azoknak az eszközöknek, politikáknak, biztonsági koncepcióknak, biztonsági intézkedéseknek, iránymutatásoknak, kockázatkezelési megközelítéseknek, cselekményeknek, képzéseknek, jó gyakorlatoknak, biztosítékoknak és technológiáknak a gyűjteménye, amelyeket fel lehet használni a kiberkörnyezet, valamint a szervezetek és a felhasználók eszközeinek védelmére."[62]

Az Európai Unió Kiberbiztonsági Stratégiája a következőképpen definiálja a fogalmat: „A kiberbiztonság azokat a biztosítékokat és intézkedéseket jelenti, amelyek segítségével mind a polgári, mind a katonai területeken egyaránt megvédhető a virtuális tér azoktól a fenyegetésektől, amelyek azok összefüggő hálózataival és információs infrastruktúráival kapcsolatosak, vagy amelyek károsíthatják ezeket." [63]

Ezek a nemzetközi stratégiák a kiberbiztonságra vonatkozó fogalmi meghatározásukkal utat mutattak Magyarország nemzeti kiberbiztonsága fő irányainak kidolgozásában, így megalkották meg 2013-ban a Nemzeti Kiberbiztonsági Stratégiát. A kormányhatározat a *kiberbiztonság* fogalmát az alábbiak szerint definiálta:„a kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez." [64] Az említett stratégiákban a közös cél a kibertér, a virtuális környezet védelme az azt fenyegető támadásoktól. Mindez a kiberbiztonság érdekében meghatározott eszközök és intézkedések alkalmazását jelenti.

8.1.8.12. Az Európai Kiberbűnözés Elleni Akciócsoport (European Cyber Crime Task Force)

Az akciócsoportot 2010-ben alakították. A szakértői csoport az Europol, az Eurojust és az Európai Bizottság képviselőiből, valamint a tagállami kiberbűnözéssel foglalkozó egységek vezetőiből áll. A csoport hozzájárul az informatikai bűncselekmények elleni küzdelem harmonizált európai megközelítésének fejlesztéséhez és támogatásához, valamint célba veszi azokat a problémákat, amelyeket az információs technológiának a bűncselekményekhez való felhasználása okoz.

8.1.8.13. Európai Multidiszciplinárius Platform a Bűnügyi Fenyegetés Ellen (European Multidisciplinary Platform Against Criminal Threats)

Az EMPACT Program lényegében az Európai Unió égisze alatt, a nemzetközi szervezett bűnözés elleni hatékony fellépés érdekében kialakított feladatrendszer, amelynek keretében több különböző prioritást (például: informatikai bűncselekmények, emberkereskedelem, szintetikus drogok, illegális migráció stb.) érintően végeznek közös munkát a kijelölt EMPACT nemzeti szakértők az EUROPOL segítségével. A kiberbűnözés keretében a cél a számítógépes bűnözés, valamint az internet bűnözési célú használata

[62] Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment and organization and user's assets.

[63] Az Európai Unió kiberbiztonsági stratégiája.

[64] Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013 (III. 21.) kormányhatározat

elleni harc. A prioritáson belül a bankkártyabűnözést, a kibertámadások elleni és a gyermekek online szexuális kizsákmányolása elleni küzdelmet fogják össze.

8.1.8.14. Eurojust

Az Eurojust szervezetét 2002-ben a Tanács 2002/187/IB határozata hozta létre, székhelye Hága. A tagállamok mindegyike egy-egy magasrangú nemzeti beosztású képviselőt delegál, akik általában bírók, ügyészek vagy hasonló hatáskörű rendőrtisztek.

Az Eurojust feladata a nemzeti nyomozó hatóságok és ügyészségek hatékonyságának növelése a határokon átívelő, súlyos és szervezett bűncselekmények ügyeiben, és végső soron annak előmozdítása, hogy a bűncselekményt elkövetők felelősségre vonása gyorsan és eredményesen megtörténjék.

Ugyanakkor a tagállamok jogrendszereinek különbözőségéből adódó nehézségeket és gyakorlati problémákat is megoldanak. A nemzeti tagokat helyetteseik, asszisztenseik és kiküldött nemzeti szakértők segítik. A harmadik államokkal – így az USA-val vagy akár Norvégiával – az Eurojust együttműködési megállapodást kötött; nekik összekötő ügyésze vagy bírója lehet az Eurojustnál, ugyanakkor az uniós jog lehetővé teszi, hogy az Eurojust összekötő ügyészt vagy bírót küldjön harmadik államokba (kölcsönösség).

Az Eurojust körülbelül 260 fős EU-személyzettel rendelkezik. Ez segíti a nemzeti hatóságok és az unió szerveinek kéréseire való gyors reagálást. Az Eurojust partnerei mind a nemzeti hatóságok, mind uniós szervezetek, mint például az Európai Igazságügyi Hálózat, az Europol, az OLAF (amennyiben az Európai Unió pénzügyi érdekeit érintő bűncselekményről van szó), a Frontex, a Sitcen, a Cepol, az Európai Igazságügyi Képzési Hálózat, továbbá minden más, a szerződések keretein belül elfogadott rendelkezések alapján kompetens szerv.

8.1.8.15. Az Interpol

Az Interpol egyik célja, hogy globális szinten összefogja és koordinálja a kiberbűncselekmények felderítését. A feladataik ellátásához megalakították a Digital Crime Centert, amely leginkább a kutatással és az innovációval kapcsolatos teendőket látja el. Ezen központ mellett létrejött még a Cyber Fusion Center, amely a szervezet tagországainak nyújt segítséget a nyomozás kezdetétől annak befejezéséig. Emellett a két egység mellett létrehozták a forenzikus tevékenységgel kapcsolatos szakértői labort is, a Digital Forensic Laboratory-t.

Az Interpol a feladata, hogy koordinálja és összehangolja a 190 tagállam közötti együttműködést a bűnüldözés területén, valamint a technológiai és technikai fejlődés figyelemmel kísérése mellett feladata a szakemberek folyamatos oktatása, felkészítése a kiberbűncselekmények változásainak megfelelően.

Felhasznált irodalom

Belegi József szerk. (2014): *Büntetőeljárás jog I–III. Kommentár a gyakorlat számára.* Budapest, HVG Orac.

Karsai Krisztina szerk. (2013): *Kommentár Büntető Törvénykönyvről szóló 2012. C. törvényhez.* Budapest, Wolters Kluwer Kiadó.

Bodor Tibor – Csák Zsolt – Somogyi Gábor – Szepesi Erzsébet – Szokolai Gábor – Varga Zoltán (2012): *Nagykommentár a büntetőeljárásról szóló 1998. évi XIX. törvényhez (Jogtár-kiegészítés).* Budapest, Wolters Kluwer Kiadó.

9. BIZONYÍTÉKSZERZÉS AZ INFORMATIKAI RENDSZEREKBŐL

Zsíros Péter

9.1.Bevezetés

A forensics tudománya egyszerűen megfogalmazva annyit jelent, hogy a bizonyítékokat olyan minőségben, és azoknak az alapelveknek a betartásával gyűjtjük össze és analizáljuk, melyek garantálják, hogy akár egy bírósági tárgyaláson is elfogadhatók lesznek. Egyáltalán nem biztos, hogy minden összegyűjtött és megvizsgált bizonyíték a bíróság elé kerül, vagy, hogy egyáltalán lesz bírósági tárgyalás. De ennek ellenére akármit is feltételezünk előre, akármilyen információt kapunk az esetleges jövőbeni felhasználásról, minden esetben úgy kell kezelni és begyűjteni a bizonyítékokat, hogy azok egyszer bizonyítási eljárásban vesznek majd részt, és végig ennek megfelelően kell kezelni azokat.

Mivel rengeteg különböző rendszer van, és mindig újabb és újabb technológiák jelennek meg, lehetetlen mindegyiket ismerni, és jelen tananyagban ismertetni. Helyette a legelterjedtebb rendszerekre koncentrálunk, illetve azokra az alapelvekre, amelyeket minden esetben alkalmazni kell.

A digitális nyomrögzítés több forrást is használ, a legfontosabb a hálózati kommunikáció, az adattárolók, a számítógépek és egyéb eszközök, például telefonok, IoT stb.

9.1.1. A legfontosabb szabályok, amelyeket be kell tartani

Bizonyíték megőrzése: ahogy az orvoslásban, itt is az első számú szabály, hogy “ne okozz kárt.” Mivel rengeteg különböző rendszer van, előbb vagy utóbb mindenkivel elő fog fordulni, hogy olyannal találkozik, amit nem ismer. Ezzel nincs semmi probléma, keressünk valaki mást, akinek már van róla tapasztalata. Egy hibás lépés a folyamat elején tönkreteheti a teljes bizonyítási eljárást, az összes későbbi munkát. A vizsgálat során mindig fontos, hogy lehetőleg ne pusztítsuk el a bizonyítékot. Ez digitális vizsgálatoknál általában könnyen megoldható, de nem mindig. Például ha szét kell szerelni egy eszközt, majd azt mi rakjuk újból össze, az már nem az eredeti állapot. Ilyen esetekben különösen ügyelni kell minden egyes lépés dokumentálására. Folyamatoknál legalább leírással és fényképekkel, de ha megoldható, videóval.

Maintain the chain of custody: a bizonyítékok átadásának és átvételének folyamata során mindig tételes jegyzőkönyvvel adjunk át mindent, és dokumentáljuk a sértetlenséget. A jegyzőkönyvet természetesen mind az átvevő, mind az átadó aláírja.

Mindent pontosan dokumentáljunk: különösen a live analízis folyamán, amikor a bizonyítékgépen dolgozunk, fontos, hogy minden kiadott parancsot, minden általunk elindított alkalmazást dokumentáljunk, hogy a memóriaanalízis során azok kivehetők legyenek a bizonyítékok közül. A dead analízis során olyan szinten szükséges a dokumentáció, hogy az alapján egy másik szakértő, a lépéseinket pontosan követve, ugyanazt az eredményt legyen képes reprodukálni.

Kövessük a szabványos eljárásokat: amennyiben léteznek szabványos, dokumentált eljárások, amelyeket szakmai testület előír, azokat kövessük. Jelen pillanatban Magyarországon nincs ilyen sza-

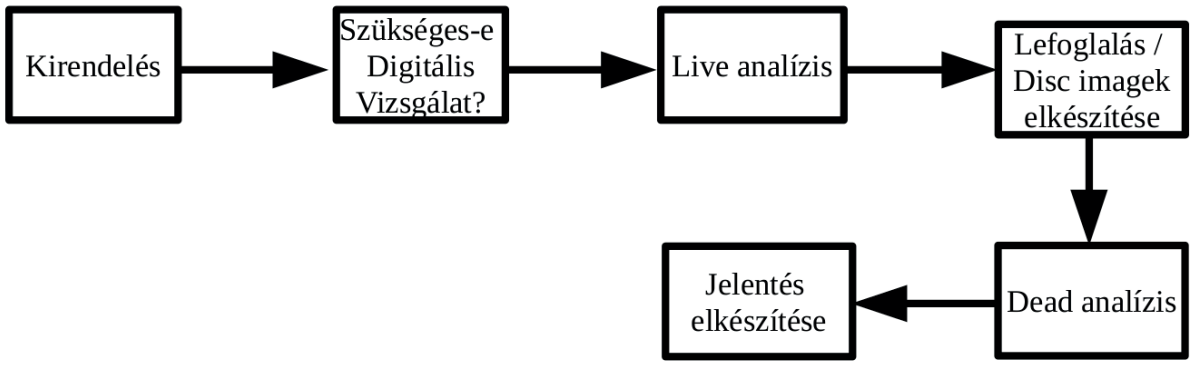
bályozás az informatikai igazságügyi szakértés területén. Ilyen esetekben a nemzetközi best practice gyakorlatokat kövessük.

9.1.2. A vizsgálat főbb lépései

Bizonyítékok megkeresése, azonosítása: sajnos minden esetben csak azzal tudunk dolgozni, ami be volt állítva az egyes rendszereknél. Például ha a logolás nem volt elég részletesen beállítva, utólag már nem lesz több log. Lehetnek olyan esetek, amikor egyszerűen a rendszerek eredeti beállítása miatt rengeteg hasznos dolog nem került megőrzésre. Ilyen esetekben a kapcsolódó rendszerekből is próbálunk keresni bizonyítékokat. A tárhelyméretek robbanásszerű növekedése miatt a bizonyítékok megkeresése egyre nehezebb.

Az események rekonstruálása a következő kérdésekre adható válaszok mentén történik: mi történt, milyen sorrendben, miért.?

Folyamat:



Forrás: A szerző saját szerkesztése

A munka egy kirendeléssel indul, mit, hol stb. kell vizsgálni.

A vizsgálat első lépése, hogy megállapítjuk, egyáltalán lehetséges-e a digitális vizsgálat. Például házkutatásnál előfordulhat, hogy nincs ott a számítógép, tehát nincs mit vizsgálni. Szintén előfordulhat, hogy minősített adatok miatt nem lehet elkezdeni az eszköz vizsgálatát. Például ügyvédi titkot érint, és nincs jelen az ügyész. Ebben az esetben meg kell várni a kiérkezését, addig a folyamat szünetel. Amikor kiérkezett, tudatjuk vele, mit fogunk tenni, és a jóváhagyásával kezdődhet a tényleges munka.

Amikor a munka megkezdődik, az első lépés, hogy eldöntsük live vagy dead analízist lehet alkalmazni. A live analízisre csak akkor kerülhet sor, ha az adott eszköz be van kapcsolva és működik. Dead analízisre minden esetben sort kerítünk a live analízis után, vagy amennyiben az nem is lehetséges, akkor helyette.

A *live analízis* annyit jelent, hogy a működés alatt álló számítógépet vizsgáljuk meg. Ez egy nagyon kritikus lépés, mert a bizonyíték azzal, hogy dolgozunk rajta, máris módosul. A lehető legkevesebb parancsot szabad kiadni, a lehető legkevesebb műveletet hajtsuk végre, csak azt tehát, ami a céljaink eléréséhez feltétlenül szükséges, és mindent dokumentáljunk. Például házkutatásnál felkérjük a felhasználót, hogy lépjen be a rendszerbe (ha belép akkor a háttérben máris lehet dokumentálni, hogy be tudott lépni, ismerte a felhasználónevet, jelszót). A futó számítógépről live analízis során az egyik legfontosabb dolog, hogy amennyiben lehetséges, teljes memóriadumpot kell készíteni. Ezt lehetőleg még a folyamat elején hajtsuk végre, hogy az általunk végzett lépések minél kevesebb memóriatartalmat módosítsanak. A vizsgált gép diszkjére minél kevesebbet (lehetőleg semmit se) írjunk. Tipikusan egy pendrive-ot csatlakoztatunk a géphez, amiről futtatjuk a memóriadumpoló alkalmazást, és ahová

mentjük az imaget. Másik lehetőség, hogy hálózaton keresztül mentsük a memóriadump tartalmát egy másik számítógépre. Ez utóbbinak az az előnye, hogy amikor USB-re mentünk, mivel az lassabb eszköz, a gép a memóriájában cachel, tehát több adatot fog megváltoztatni. Hátránya, hogy a hálózati beállítások módosulnak, a hálózati kábelt lehet, hogy ki kell húzni, aminek a hatására a gép már töröl néhány memória cache-t.

Ha lehet, az adatok lekérdezését parancssori alkalmazásokkal végezzük, mert kisebbek, így kevesebb bizonyítékot módosítanak, mint a grafikus alkalmazások.

Amit még javasolt menteni: hálózati beállítások, DNS cache (ipconfig /displaydns), ARP cache (arp -a), process lista (tasklist /svc, tasklist /M), teljes fájllista (dir /r /s c:\), registry (reg save), gépen beállított idő eltérése a valódi időhöz képest (time /t), időzóna, operációs rendszer (ver), servicepack verzió. Ezek azért jók, hogy a felhasználó nézőpontjából is megvizsgálhassuk, mit látott a gépen, például ha rootkit, malware elrejtett valamit, és azt a felhasználó nem láthatta.

Lefoglalás: A live analízis után a következő lépés a gép lefoglalása. El kell döntenünk, hogy az egész gépet fizikailag lefoglaljuk, vagy a diskről készítünk megfelelő forensics imaget. Amennyiben lehetséges, törekedni kell, hogy ne kelljen a fizikai gépet lefoglalni, az esetleges későbbi kártérítési pereket elkerülendő. Természetesen itt figyelembe kell venni, mennyi ideig fog tartani az image elkészítése, lehet, hogy ott helyben időhiány miatt nem kivitelezhető. Szintén vegyük figyelembe, amennyiben valamilyen raid rendszer van, például raid0 vagy raid5, ez inkább vállalati rendszereknél fordulhat elő, azt utána nehéz ismét összeállítani, ezért minél több információt tudjunk meg a raidről. A lefoglalás során a BIOS beállításait (a disk kiszerelése után, nehogy véletlenül beindítsuk a gépet, és így bizonyítékok semmisüljenek meg) rögzítsük, legegyszerűbb fényképpel. A BIOS időeltérését a valódi időhöz képest szintén rögzítsük. A disk kiszerelését részletesen dokumentáljuk, a gép minden részéről, csatlakoztatott kábelekről, sorozatszámokról készítsünk fényképet.

Dead analízis: A lefoglalt anyagokat (disk image, memória image, számítógép) analizáljuk.

A kapott eredmények alapján elkészítjük a jelentést.

9.2. Lefoglalás (Acquire)

9.2.1. Szükséges eszközök

Mivel a lefoglalás könnyen elképzelhető, hogy a helyszínen zajlik, így alaposan fel kell készülni előre, mert nem valószínű, hogy bármilyen szükséges eszközt a helyszínen még be lehet szerezni. Amik mindenképpen szükségesek:

- csavarhúzó készletek;
- merevlemez-adatkábelek és konverterek;
- kiszerelt merevlemezek meghajtásához tápok, különböző tápcsatlakozókkal;
- írásblokkolók a különböző csatlakozó típusokhoz, esetleg másolóberendezés, forensics laptop;
- zseblámpa, nagyító (sorozatszám néha nehezen olvasható);
- sűrített levegő (néha porréteg takarja az egyedi azonosító számokat);
- merevlemezek, egyéb tárolók a másolatoknak;
- USB kulcsok a szükséges alkalmazásokkal, megírt scriptek, hogy gyorsabban tudjunk dolgozni, és elegendő szabad tárhellyel memória imagehez. (különböző operációs rendszerekhez és architektúrákhoz külön USB kulcsok, felcímkézve, hogy tudjuk, melyik melyikhez való);
- fényképezőgép, videókamera;
- mobilinternet, ha valaminek utána kell nézni;
- UTP kábelek, cross kábel (bár a gigabites ethernet szabvány szerint nincs már rá szükség, de még találkozhatunk gépekkel, amiken csak 100 Mbit-es ethernet port van), switch, wireless AP, ha csak wifi van az eszközön például laptop;

- CD-, DVD-, Blueray- stb. olvasó;
- memóriakártya-olvasó.

Amennyiben rendelkezünk másolóeszközzel, azzal a másolás sokkal gyorsabb és egyszerűbb, valamint hasznos, ha eleve rendelkezik beépített írásblokkolóval is. Csatlakoztatjuk a forrásoldalra a vizsgálandó gépből kiszerelt merevlemezt, a céloldalra pedig a célmerevlemezt. Ezután eszköztől függően pár gombnyomás, és a másolás elkezdődik. Ennek a módszernek az előnye a gyorsaság, a kényelem, az egyszerűség. Hátránya az ilyen eszközök ára (a másolóeszközök ára nagyságrendileg 300 ezer forint környékén kezdődik, és határ a csillagos ég). Ilyen berendezések bérelhetők is, ebben az esetben előtte próbáljuk ki az eszközt, hogy tudjuk, hogyan működik.

Amennyiben nem rendelkezünk másolóeszközzel (mert az csak akkor kifizetődő, ha sok ilyen munkát kell végezni), mindenképpen használjunk írásblokkolót a másolat elkészítéséhez. Írásblokkolókból sokféle van, áruk pár tízezer forinttól indul. Különböző csatlakozótípusokhoz lehet írásblokkolót venni. Mivel legvalószínűbb, hogy USB porton keresztül másolunk, ezért legcélszerűbb olyat vásárolni. Akkor egyúttal a konvertert is megoldottuk, ugyanis lehet olyan írásblokkolót kapni, amelynél a forrásoldal többféle lehet (SATA, SCSI, SAS stb.), a céloldal pedig USB. USB esetében mindenképpen igyekezzünk legalább 3.0 USB verziót használni, mert jelentős a sebességkülönbség.

Utolsó lehetőségként, amennyiben semmilyen fizikai írásblokkolónk nincs, logikailag blokkoljuk az írást a saját forensics laptopunkon, az adott USB portra udev szabályok készítésével.

9.2.2. A memóriatartalom mentése

Live analízis során alapvető lépés a teljes memóriatartalom elmentése, amit utána analizálni tudunk. Ez nem túl egyszerű feladat. Valójában, ha rootkit vagy malware van a számítógépen, azok elképzelhető, hogy egy memória image-ben sem jelennek meg. Egy rootkit képes lehet rá, hogy a virtual memory manager-re való hookolással megváltoztatott memóriatartalmat mutasson, amikor az adott tartományt (ahol ő maga van) csak olvassák. Emiatt a memóriatartalom mindig lehet megváltoztatott, de ennek nyilván nagyon minimális az esélye, ilyen bonyolultságú rootkit elkészítése stabilra különböző operációs rendszerekre rendkívül nehéz feladat, inkább speciális, célzott támadásoknál fordulhat csak elő.

A memória tartalmát nagyon sokféle alkalmazással lehet menteni, több alkalmazás legyen nálunk, és mindig legyünk naprakészek, hogy melyik alkalmazás melyik verziója milyen operációs rendszeren működik. A működést tesztkörnyezetben ellenőrizzük. Az újabb verzió nem biztos, hogy jobb, elképzelhető, hogy régebbi operációs rendszerekre már nem működik, ezért mindig tartsuk meg a bevált változatokat is, és csak alapos tesztelés után cseréljük le őket. Az új változatnak könnyen elképzelhető, hogy más kapcsolói kellenek, ezt is ellenőrizzük használat előtt. Az ellenőrzéskor mindig próbáljuk ki, hogy az analizáló alkalmazás tudja-e használni az elkészült image-t, ugyanis könnyen előfordulhat, hogy elkészül a memóriadump, boldogok vagyunk, de amikor analizálná valaki, kiderül, hogy mégsem jó a formátum. Az elkészült imagen legalább egy alaplekérdezést futtassunk le, hogy valóban használható-e. A leggyakrabban használt memóriaanalizáló alkalmazás a volatility, ezért érdemes ezzel tesztelni.

Nem minden memóriát imagelő alkalmazás készít hash értéket, ezért mindenképpen legyen hash számoló program, és amennyiben olyan alkalmazást használunk, akkor az elkészülte után a memóriadumpfájlról azonnal készítsünk hash-t is, amit természetesen szintén rögzítsünk a jegyzőkönyvben is, csakúgy, mint a merevlemez-tartalom imagelésénél tettük.

A memóriadumpoló alkalmazások egy része lehetőséget ad a page fájl mentésére is. Lehetőség szerint használjuk ezt az opciót, mert a page fájlban is sok hasznos információ van. Ezt természetesen megkapjuk a disk imagelési eljárással is, de akkor két külön fájlunk van, amit a memóriaanalizáló alkalmazásnak oda kell adni, kicsit kényelmetlenebb úgy használni.

9.2.2.1. Windowsos gép memóriatartalmának mentése DumpIt alkalmazással

A DumpIt alkalmazás segítségével többféle formátumban készíthetünk memóriaimaget. Ezek a raw, vagy dmp, a default a dmp formátum. Az alkalmazás egyből készít egy SHA256 hashértéket is, a dump elkészülte után ezt vegyük jegyzőkönyvbe.

Sajnos azonban a page fájlt nem tudja menteni és beletenni a memóriadumpba, azt külön kell kezelni.

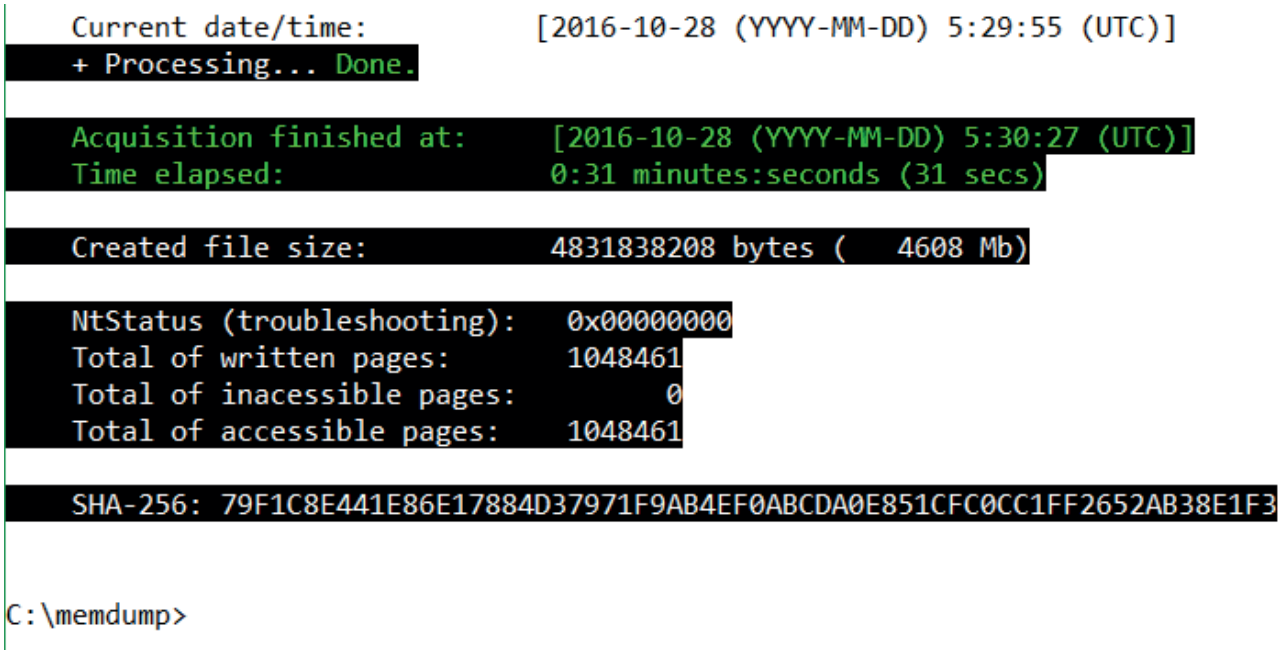
Amennyiben raw formátumot készítünk, azt a volatility nem képes megfelelően használni, konverziók szükségesek:

```
C:\memdump>DumpIt.exe /T RAW /o b.dmp

  DumpIt 3.0.109.20161007
  Copyright (C) 2007 - 2016, Matthieu Suiche <http://www.msuiche.net>
  Copyright (C) 2012 - 2014, MoonSols Limited <http://www.moonsols.com>
  Copyright (C) 2015 - 2016, Comae Technologies FZE <http://www.comae.io>

    Destination path:           \??\C:\memdump\b.dmp

    Computer name:              ATTACKER2K16


    --> Proceed to the acquisition ? [y/n] y

    [+] Information:
    Dump Type:                   Raw Memory Dump


    [+] Machine Information:
    Windows version:            10.0.14393
    MachineId:                  90B42F09-56F4-254D-B38D-B1704E88B035
    TimeStamp:                  131221061952902862
    Cr3:                        0x1aa000
    KdCopyDataBlock:            0xfffff803445ebff4
    KdDebuggerData:             0xfffff8034470c500
    KdpDataBlockEncoded:        0xfffff8034475c110
```

1. ábra

DumpIt használata

Forrás: A szerző saját szerkesztése

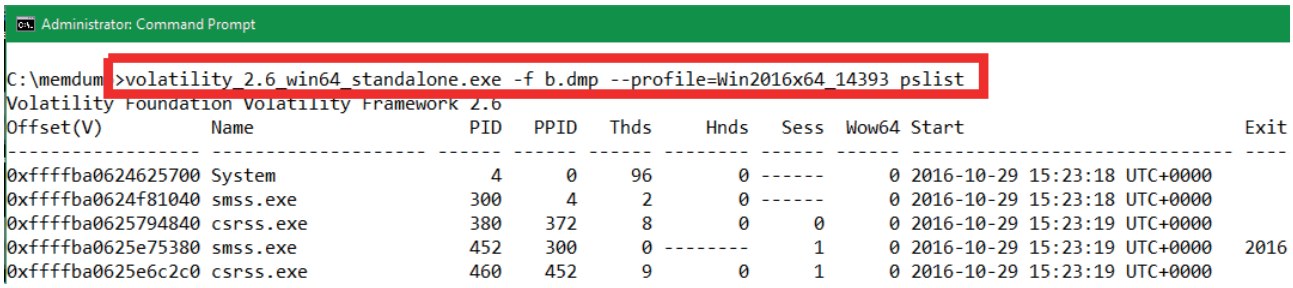


2. ábra

DumpIt használata

Forrás: A szerző saját szerkesztése

Ellenőrizzük az elkészült dumpot, hogy használható-e. Ehhez a volatility alkalmazást használjuk. Először is meg kell állapítani, milyen operációs rendszerről készítettük az imaget. Ezt a helyszínen a ver paranccsal könnyen meg tudjuk tenni, ez volt az egyik javasolt parancs, amit futtatni kell live analízis során. Majd adjunk ki valami egyszerű parancsot például: volatility -f <image file neve> --profile=Win2016x64_14393 pslist. Amennyiben a parancs sikeresen lefut, használható az image. A profil megadásánál vigyázzunk, mert kis- és nagybetűre érzékeny.

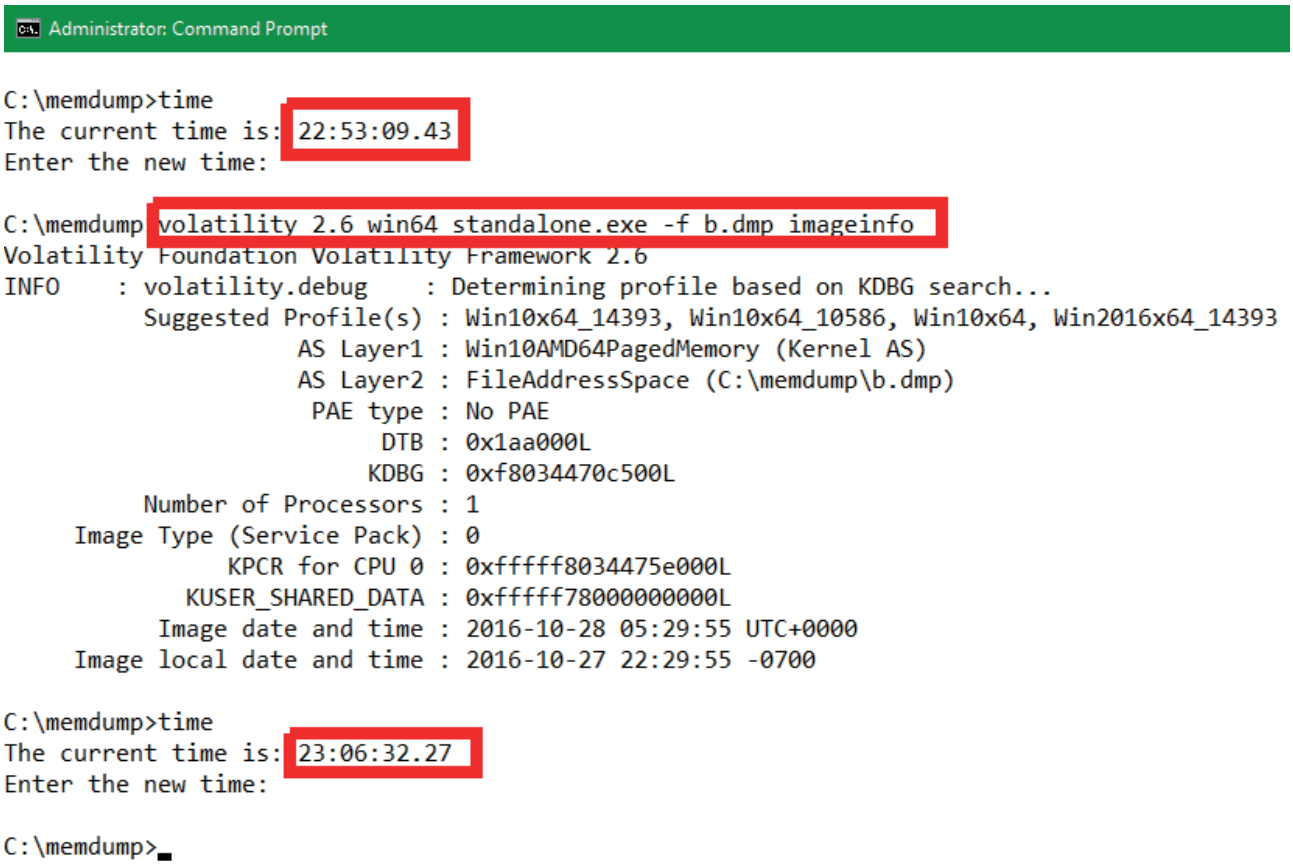


3. ábra

Az elkészült dump használhatóságának ellenőrzése egy egyszerű paranccsal

Forrás: A szerző saját szerkesztése

Amennyiben utólag analizáljuk az imaget, az operációs rendszer verzióját a volatility -f <image file neve> imageinfo paranccsal tudjuk lekérdezni. Ezután, mint korábban, a --profile= kapcsolóval tudjuk megadni. Ez nagyon fontos lépés, mert az oprendszer megállapítása sokáig tart, 4GB memóriánál 10–15 perc is lehet. Amennyiben nem adjuk meg a volatility meghívásakor a profilt, akkor minden egyes parancs végrehajtása előtt külön meg kell állapítani az oprendszert, igy rengeteg időt veszítünk. Másik probléma, hogy számos parancs, például az imént használt pslist is, hibásan futhat, ha nem adjuk meg neki a profilt.

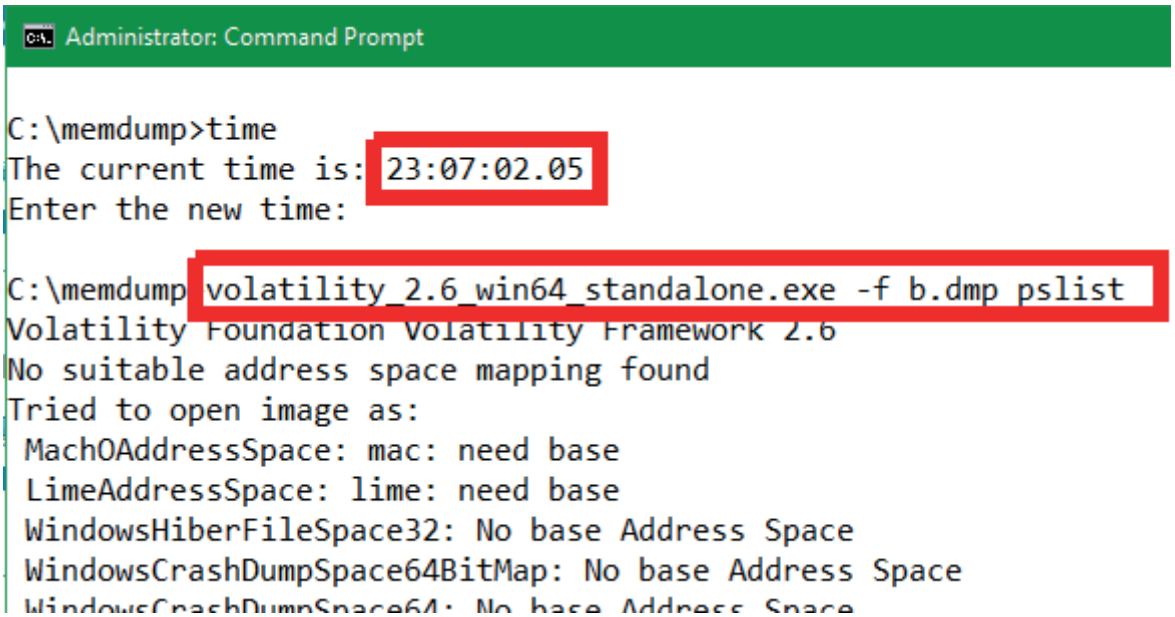


4. ábra

Az operációs rendszer verziójának lekérdezése a volatility -f <image file neve> imageinfo paranccsal

Forrás: A szerző saját szerkesztése

Hibásan futó pslist parancs ugyanerre az image-re:



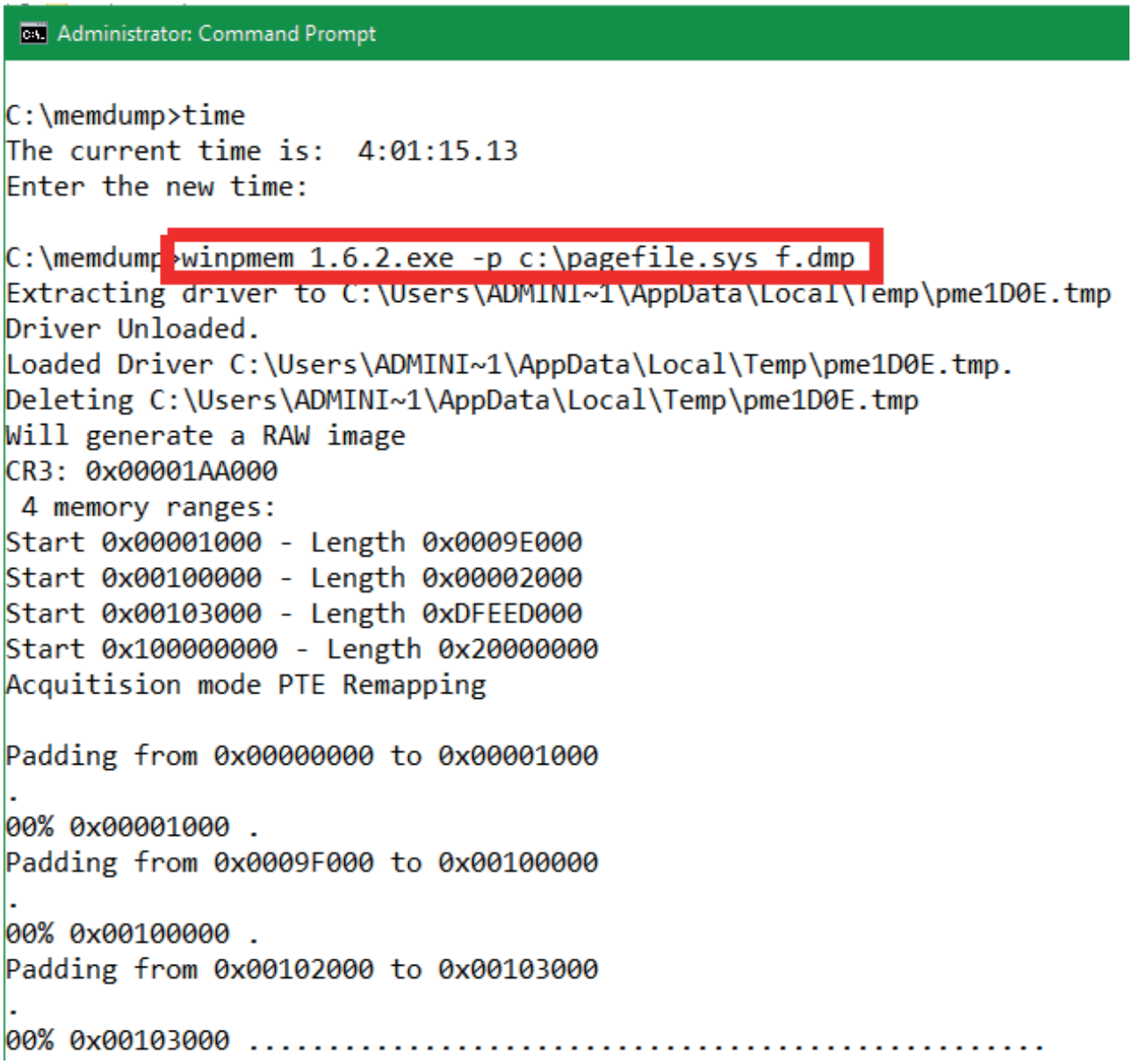
5. ábra

Hibásan futó pslist parancs

Forrás: A szerző saját szerkesztése

9.2.2.2. Windowsos gép memóriatartalmának mentése Winpmem 1.6.2 alkalmazással

Másik elterjedt alkalmazás memóriadump készítésére a winpmem, amelyből többféle verziót is találunk. Alapból sajnos nem készít hashértéket, azt külön kell számíttatnunk. Képes a pagefájl mentésére a -p kapcsoló használatával.



```
98% 0x11C200000 ..................................................
99% 0x11F400000 ............
Driver Unloaded.

C:\memdump>time
The current time is:  4:01:37.11
Enter the new time:

C:\memdump>
```

6. ábra

Winpmem használata

Forrás: A szerző saját szerkesztése

9.2.2.3. Windowsos gép memóriatartalmának mentése Winpmem 2.1 alkalmazással

Az újabb verzió rengeteg új kapcsolóval bővült, és számos új formátumot támogat, ami macerásabbá is teszi a használatot. Az alapértelmezett beállításokkal készített mentés például nem használható volatilityvel. Ez azért van, mert zippelt AFF4 formátumban ment alapból. Az AFF4 több adatstreamet tartalmaz, és azok közül csak egy a memóriadump, amire a volatilitynek szüksége van, ezért kicsit összezavarodik. Ha volatilityvel akarjuk használni, akkor alkönyvtárba mentsünk, ne fájlba (vagy a kapott zip fájlt utána csomagoljuk ki egy alkönyvtárba). A formátumot állítsuk elf vagy raw formátumra (Winpmem-2.1 --format elf -o .\x\)

```
Administrator: Command Prompt

C:\memdump>winpmem-2.1.post4.exe --format elf -o .\x\
Driver Unloaded.
CR3: 0x00001AA000
 4 memory ranges:
Start 0x00001000 - Length 0x0009E000
Start 0x00100000 - Length 0x00002000
Start 0x00103000 - Length 0xDFEED000
Start 0x100000000 - Length 0x20000000
E1029 03:07:34.010674  1272 aff4_file.cc:138] Can not open file C:\mem
E1029 03:07:34.010674  1272 aff4_file.cc:138] Can not open file C:\mem
Creating output AFF4 Directory structure.
Dumping Range 0 (Starts at 1000, length 9e000)
```

7. ábra

A helyes formátum beállítása

Forrás: A szerző saját szerkesztése

```
Adding C:\Windows\SysNative\drivers\xinputhid.sys as file:///C:/Windows/SysNative/drivers/xinputhid.sys
Adding C:\Windows\SysNative\ntoskrnl.exe as file:///C:/Windows/SysNative/ntoskrnl.exe
Driver Unloaded.

C:\memdump>
```

Mivel az alkalmazás nem számolt hashértéket, egy külön lépésben számoltassunk az elkészült alkönyvtárra, és rögzítsük a jegyzőkönyvben.

Ezután ellenőrizzük a volatility-vel, hogy használható-e a dump.

```
Administrator: Command Prompt
C:\memdump>volatility_2.6_win64_standalone.exe -f x\PhysicalMemory --profile=Win2016x64_14393 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ----
0xffffba0624625700 System                    4      0     96        0 ------      0 2016-10-29 15:23:18 UTC+0000
0xffffba0624f81040 smss.exe                300      4      2        0 ------      0 2016-10-29 15:23:18 UTC+0000
0xffffba0625794840 csrss.exe               380    372      8        0      0      0 2016-10-29 15:23:19 UTC+0000
0xffffba0625e75380 smss.exe                452    300      0 --------      1      0 2016-10-29 15:23:19 UTC+0000   2016
0xffffba0625e6c2c0 csrss.exe               460    452      9        0      1      0 2016-10-29 15:23:19 UTC+0000



0xffffba06263cd080 VBoxTray.exe           3428   3000     10        0      1      0 2016-10-29 06:26:15 UTC+0000
0xffffba0626095540 winpmem-2.1.po         2196   3320      2        0      1      0 2016-10-29 10:07:33 UTC+0000

C:\memdump>
```

8. ábra

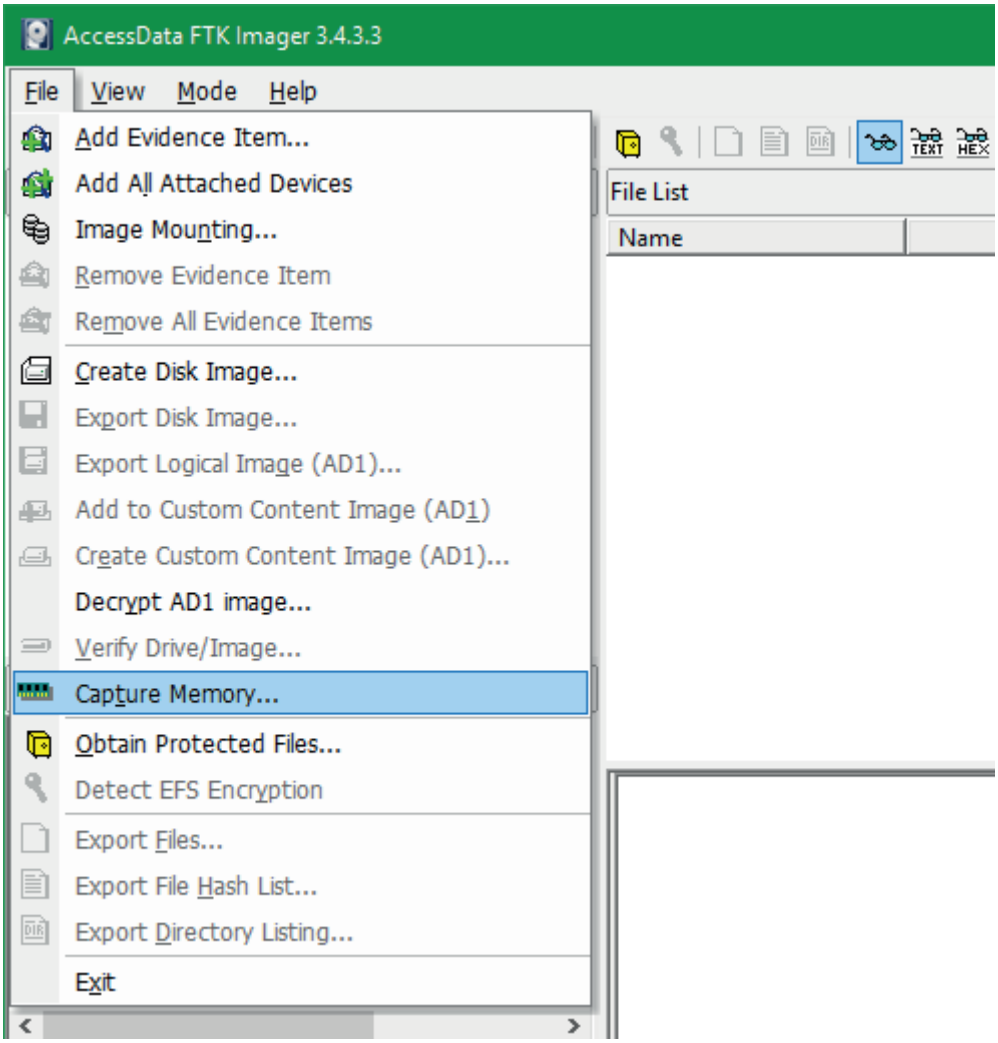
A dump használhatóságának ellenőrzése volatility-vel

Forrás: A szerző saját szerkesztése

9.2.2.4. Windowsos gép memóriatartalmának mentése FTK imager alkalmazással

Az FTK, a „The Forensic Toolkit” egy elterjedt alkalmazás, amelynek van egy ingyenesen letölthető és használható imager része (a legtöbb fizetős alkalmazásra igaz, hogy a hozzá tartozó imagekészítő ingyenesen elérhető, hiszen a gyártónak is érdeke, hogy minél többen az ő formátumában csinálja az imaget). A tool képes többek között a disk és a memória imagelésére is. Alapértelmezés szerint sajnos telepíteni kell, de ha saját gépre telepítjük, majd a binárisokat lemásoljuk, működni szokott pendrive-ról is. Azonban itt azért előjöhetnek hiányzó dll dependenciák vagy egyéb gondok, ezért célszerű mellette mindig tartani alternatív megoldást. A bizonyítékgépre ne telepítsük. Előnye, hogy kényelmes, könnyen használható grafikus alkalmazás. Mivel egy elterjedt fizetős termék része, rendszeres és megbízható a frissítése, az új operációs rendszerek követése. Képes a pagefájl mentésére is, tehát javasolt élni a lehetőséggel. Hátránya, hogy mivel grafikus alkalmazás, nagyobb méretű, mint az eddigiek, tehát több dolgot változtat a bizonyítékgép memóriájában. Sajnos nem számol hashértéket azonnal, azt egy külön körben kell végrehajtanunk. A volatility képes használni az alapértelmezés szerint készített memóriadumpját.

Használatához indítsuk el az FTK imager alkalmazást, majd válasszuk a „Capture Memory” menüpontot.

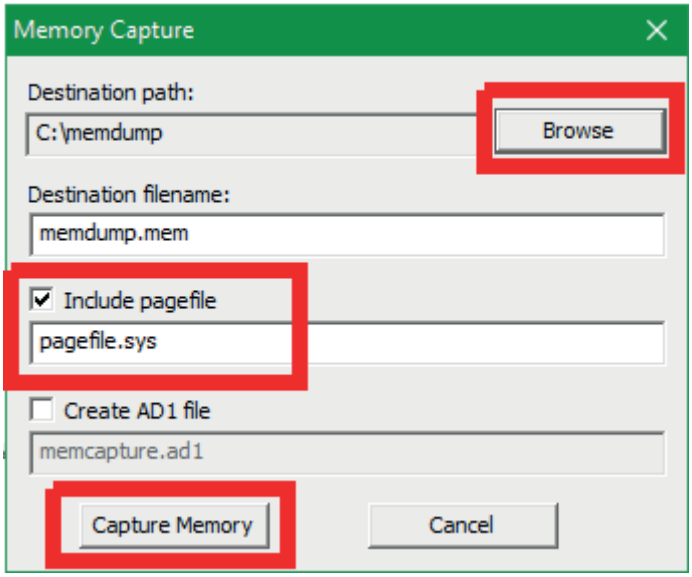


9. ábra

Az FTK imager alkalmazás indítása

Forrás: A szerző saját szerkesztése

A megjelenő új ablakban adjuk meg a mentés helyét, lehetőleg mentsük a pagefájlt is, majd kattintsunk a Capture Memory gombra.

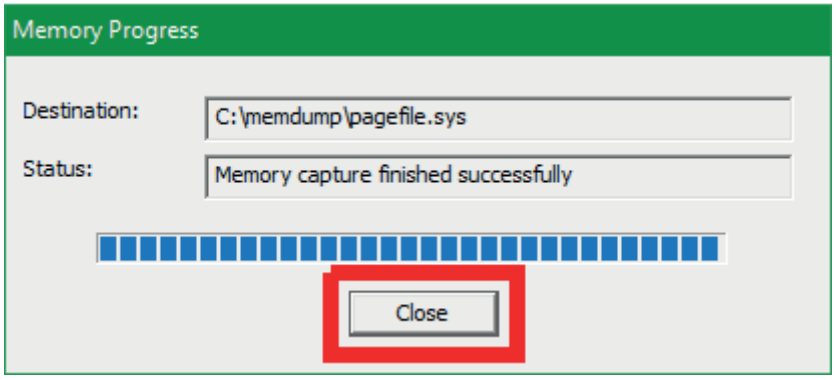


10. ábra

A pagefájl mentése

Forrás: A szerző saját szerkesztése

Várjuk meg, amíg befejezi a dumpolást, majd kattintsunk a Close gombra.

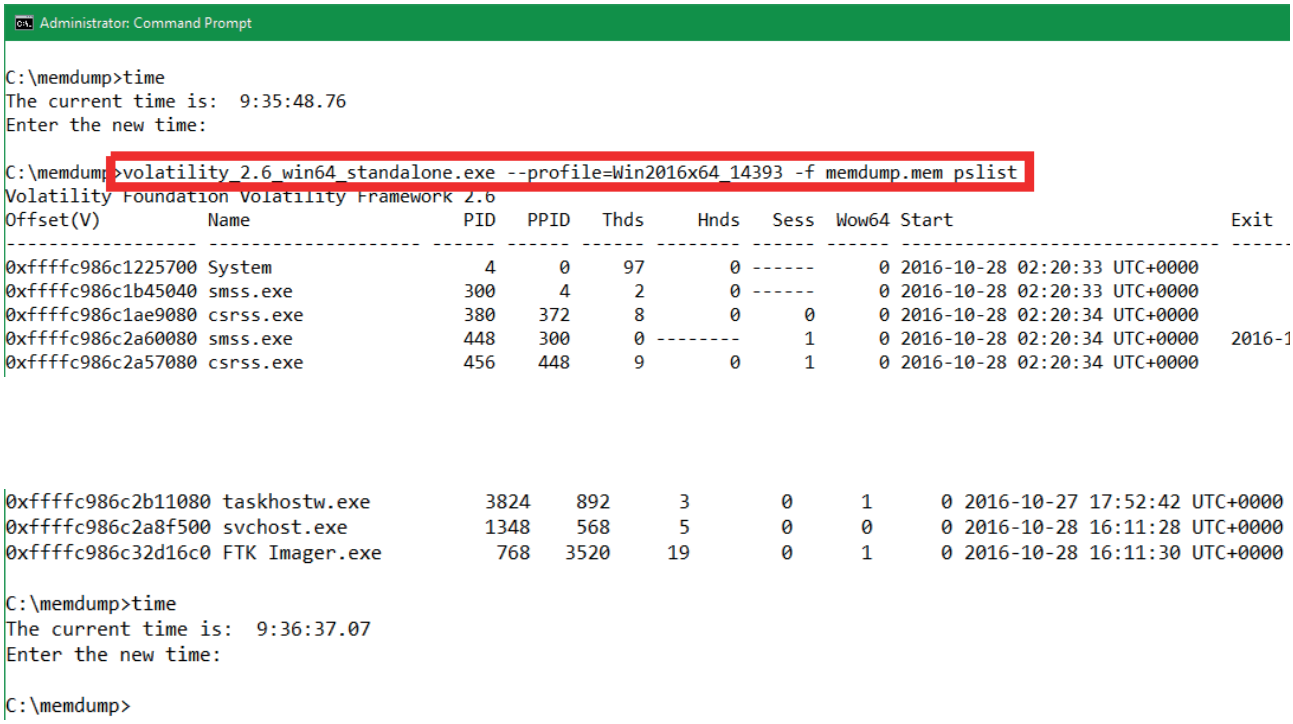


11. ábra

A dumpolás befejezése

Forrás: A szerző saját szerkesztése

Ezután számítsuk ki, és vegyük jegyzőkönyvbe a hashértéket, és rögzítsük a jegyzőkönyvbe. Majd ellenőrizzük a volatility-vel, hogy használható-e a dump.



12. ábra

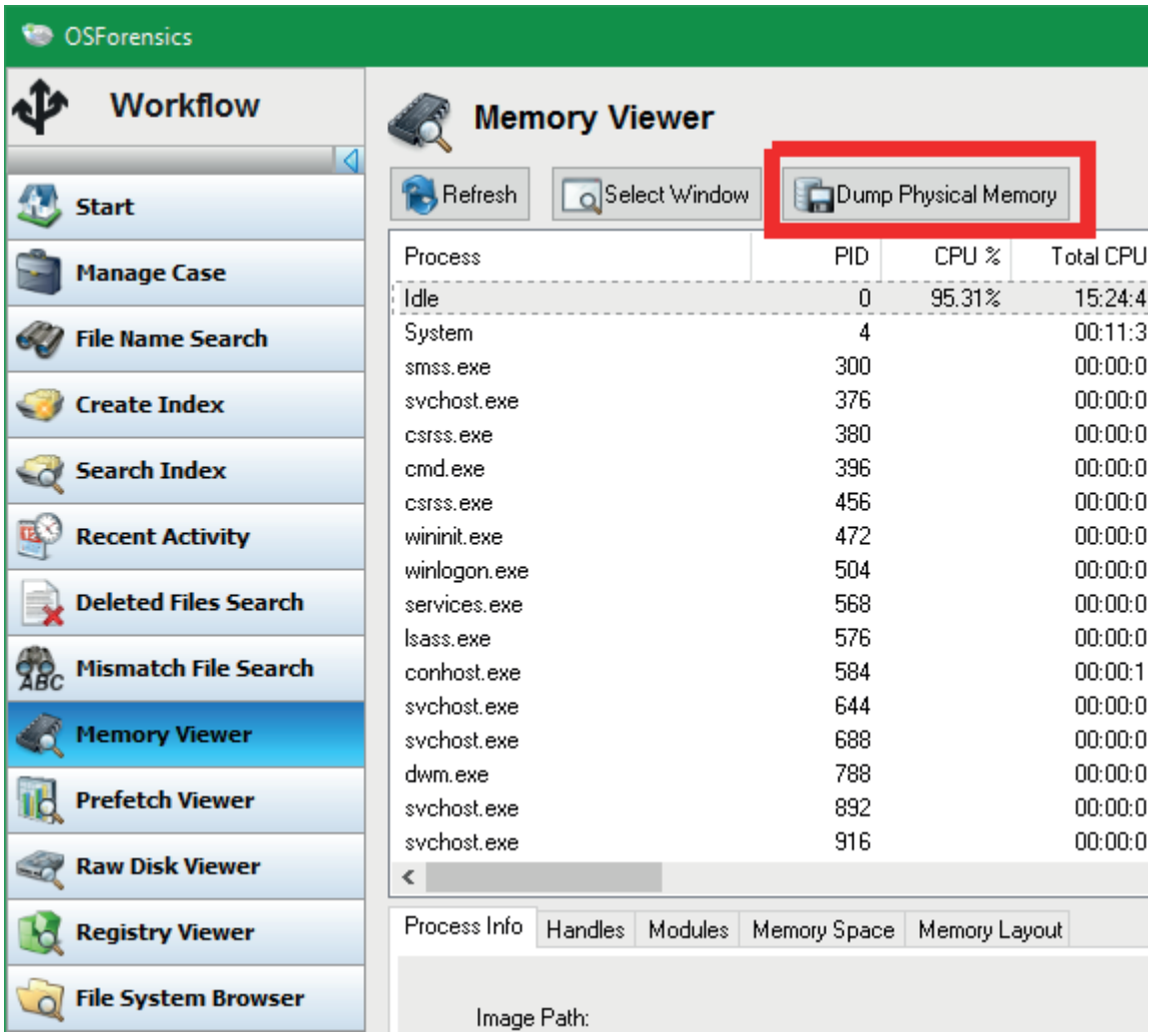
A dump ellenőrzése a volatility-vel

Forrás: A szerző saját szerkesztése

9.2.2.5. Windowsos gép memóriatartalmának mentése OSF programmal

Az OSF az OS Forensics nevű ingyenes forensics analizáló program futtatható állománya. Csakúgy, mint az előző FTK imager, ez is alapvetően egy telepítést igénylő alkalmazás, de ha saját gépre telepítjük, van egy „copy to usb” menüpontja, ami a binárisokat lemásolja egy pendrive-ra. Ez nagy valószínűséggel megfelelően fog futni a vizsgálandó gépen. Szintén képes többek között diszk és memóriaimage készítésére, de azonkívül egy teljes analizáló környezet is. Amennyiben egy egyszerűbb, all in one grafikus alkalmazást szeretnénk használni a parancssori eszközök helyett, akkor jó választás lehet számunkra.

Amennyiben memóriadumpot akarunk készíteni, válasszuk a *Memory Viewer* részt a *workflow*-ból, majd kattintsunk a *Dump Physical Memory* gombra.

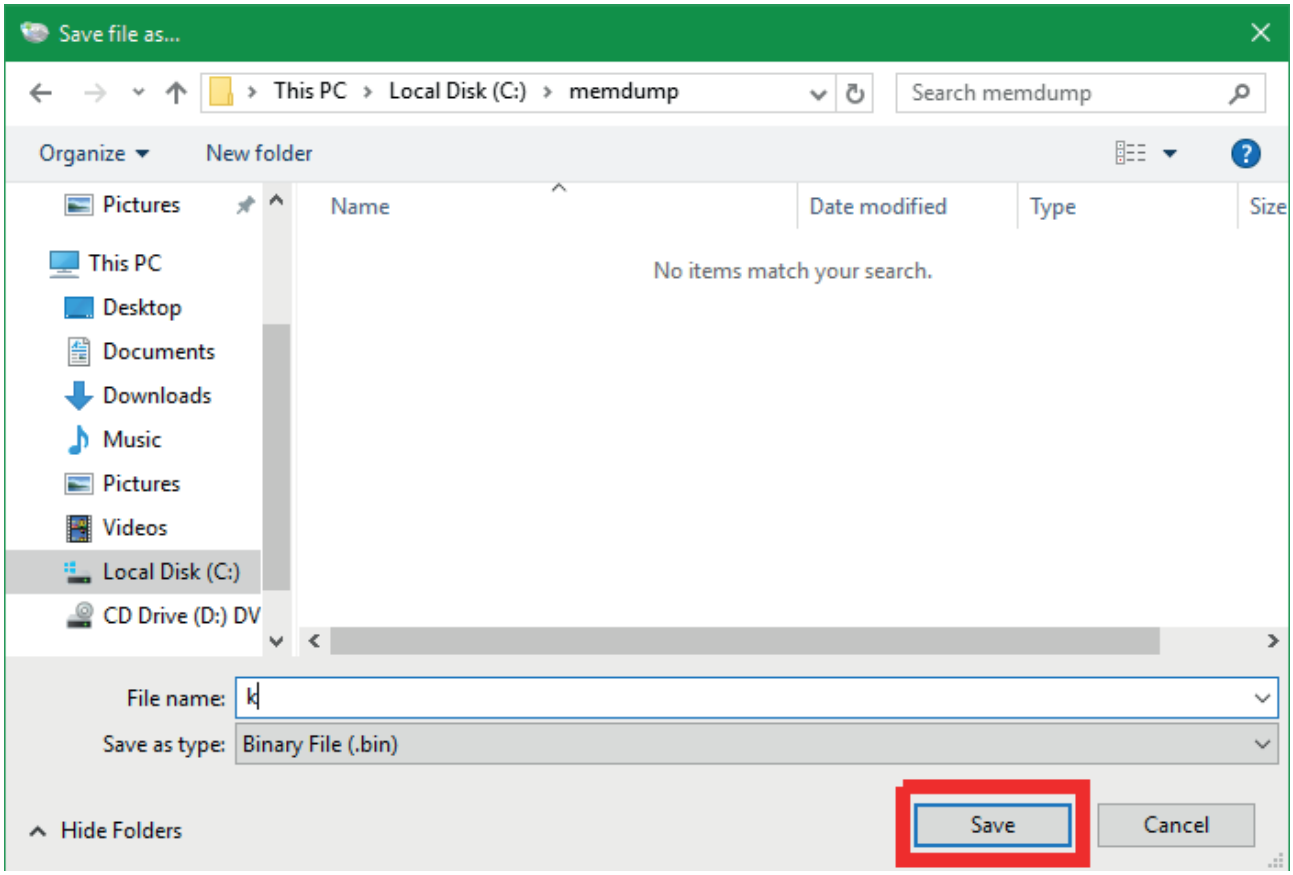


13. ábra

Memóriadump készítése OSF programmal

Forrás: A szerző saját szerkesztése

A megjelenő „save file” párbeszédablakban adjunk nevet a fájlnak, majd kattintsunk a save gombra.

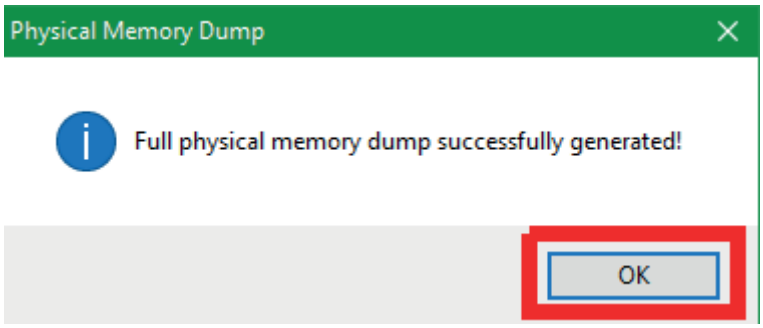


14. ábra

Mentés az OSF programban

Forrás: A szerző saját szerkesztése

Várjuk meg, amíg a dump elkészül, majd kattintsunk az OK gombra.

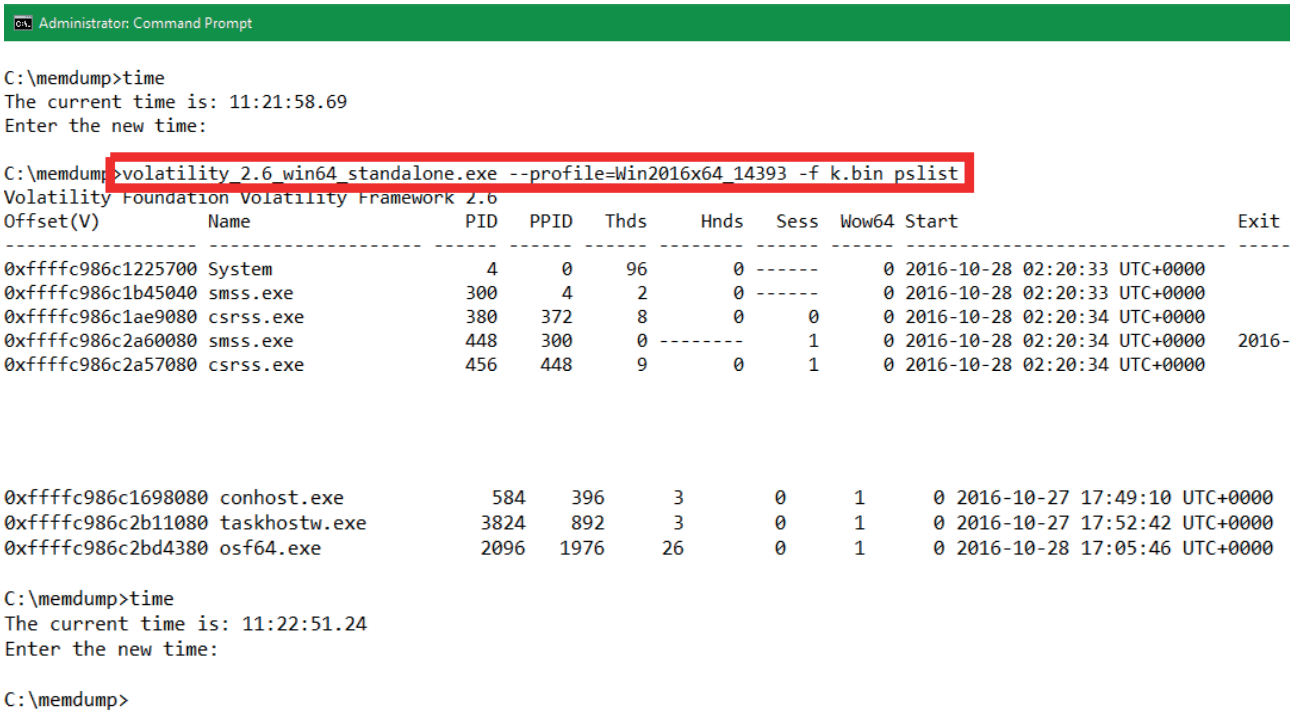


15. ábra

A memóriadump elkészítése OSF programmal

Forrás: A szerző saját szerkesztése

Szintén nem készít hash-t alapból, úgyhogy azt külön lépésként tegyük meg, majd jegyzőkönyvezzük az értéket. Ezek után ellenőrizzük az elkészült imaget volatility-vel, hogy használható-e.



16. ábra

Az elkészült dump ellenőrzése volatility-vel

Forrás: A szerző saját szerkesztése

*9.2.2.6. *Nix alapú gép memóriatartalmának mentése*

Valamikor a régi időkben a linuxos gépek memóriatartalmának a dumpolása sokkal egyszerűbb volt, mint a windowsos gépeké. Létezett egy /dev/mem nevű device, amely a fizikai memóriához nyújtott hozzáférést, illetve egy /dev/kmem nevű, amely a virtuális memóriatartalmat mutatta. Ezek a fájlok modern nixes rendszereken már nem léteznek, mivel hasznosak voltak ugyan forensics szempontból, de irtózatos biztonsági rést jelentettek, hiszen egy user módú device segítségével a teljes memóriát el lehetett érni. Még ha léteznének, akkor is lenne egy olyan limitáció, hogy a /dev/mem csak a fizikai memória első 896 MB-ját mutatta. Ezért ma már ezeket nem tudjuk használni. Helyette a következő megoldások alakultak ki.

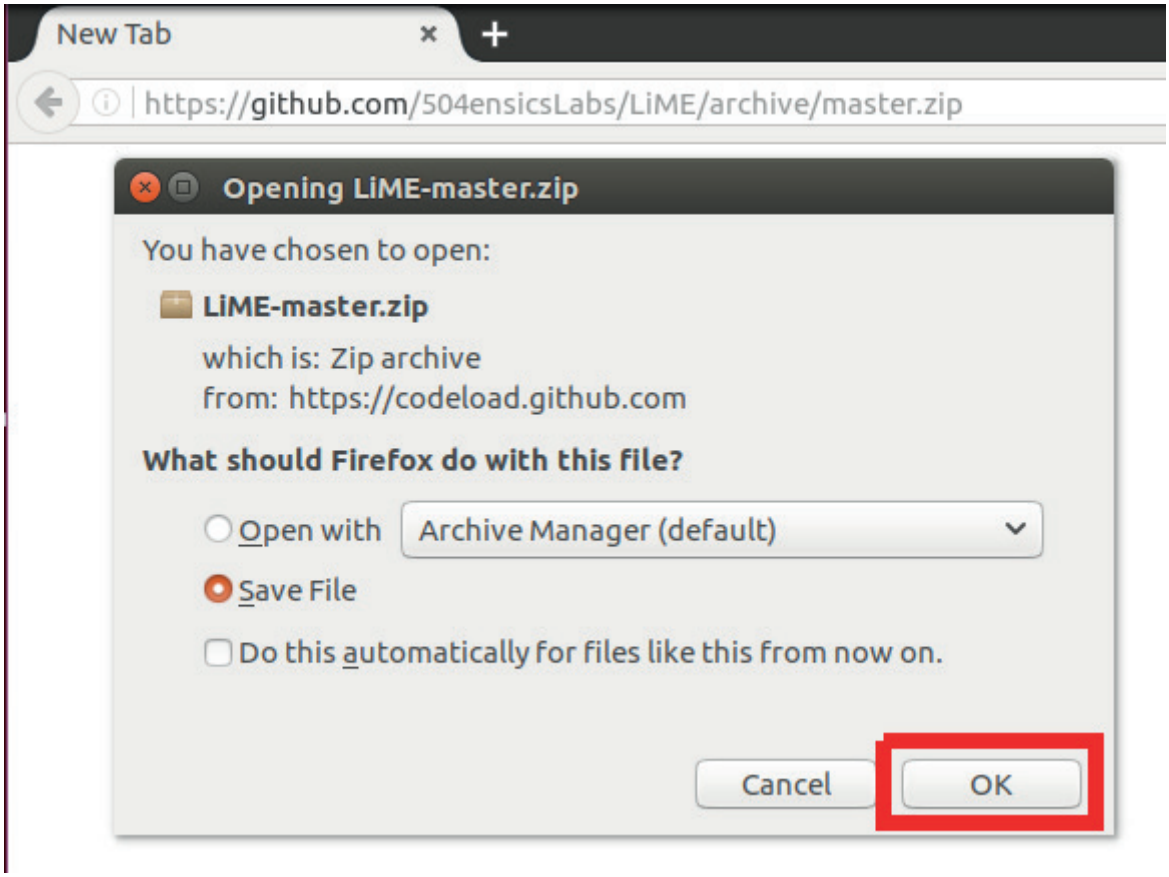
*9.2.2.7. *Nix alapú gép memóriatartalmának mentése Fmem és Forensics Memory eszközökkel*

Ez a nehézkesebb megoldás. Segítségével egy, a régi dev/mem-hez hasonló eszközt kapunk. Erről például dd segítségével készíthetünk másolatot. Sajnos a másolat használata nem olyan egyszerű, mert volatility-vel és egyéb eszközökkel nem használható, nem memóriadump-formátum, hiányoznak a szükséges metaadatok.

*9.2.2.8. *Nix alapú gép memória tartalmának mentése LiMe és Linux Memory Extractor eszközökkel*

Ez a javasolt megoldás. Az alkalmazás ubuntu alapú rendszerekre egyszerűen telepíthető az apt-get install lime-forensics-dkms parancs segítségével.

Saját laptopról használva, az alkalmazást újra kell fordítanunk a vizsgálandó rendszer kernelverziójához, ezért inkább töltsük le a forrást a https://github.com/504ensicsLabs/LiME címről, majd a binárist kell áttennünk a célgépre.



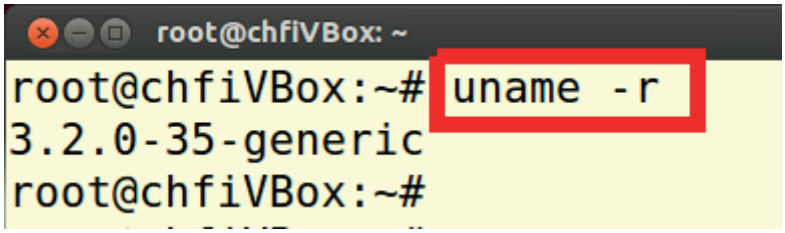
17. ábra

A LiME eszköz működtetése

Forrás: A szerző saját szerkesztése

Mivel rengeteg féle linux kernelverzió van, és rendszeresen jönnek ki újabbak, lényegében lehetetlen, hogy minden kernelverzióra fordított példány nálunk legyen. Helyette az úgynevezett cross compile szükséges, ami azt jelenti, hogy az egyik linux kernelverzión egy másik kernelverzióra fordítunk. Az ilyesmi rettenetesen macerás tud lenni, újabb gcc verzió már nem támogat kapcsolókat, vagy alapbeállítás eltérések miatt plusz kapcsolókat kell betenni. Mindenképpen arra készüljünk, hogy sok problémával jár. Ennek elkerülése érdekében célszerű a forensics laptopon virtuális gépben tartani legalább kb. 8–12 évre visszamenőleg az összes LTS (Long Time Support) linuxverziót (4–6 virtuális gép), és a cél operációs rendszerhez legközelebb eső verziókkal megpróbálni először a fordítást. Ez rengeteg problémától kímélhet meg minket, és sokkal gyorsabbá teheti a munkát. Most mindenesetre bemutatom a cross compile-t, ami a következő folyamatból áll:

Megnézzük a vizsgálandó gép kernel verzióját az uname -r paranccsal



18. ábra

Az uname-parancs használata

Forrás: A szerző saját szerkesztése

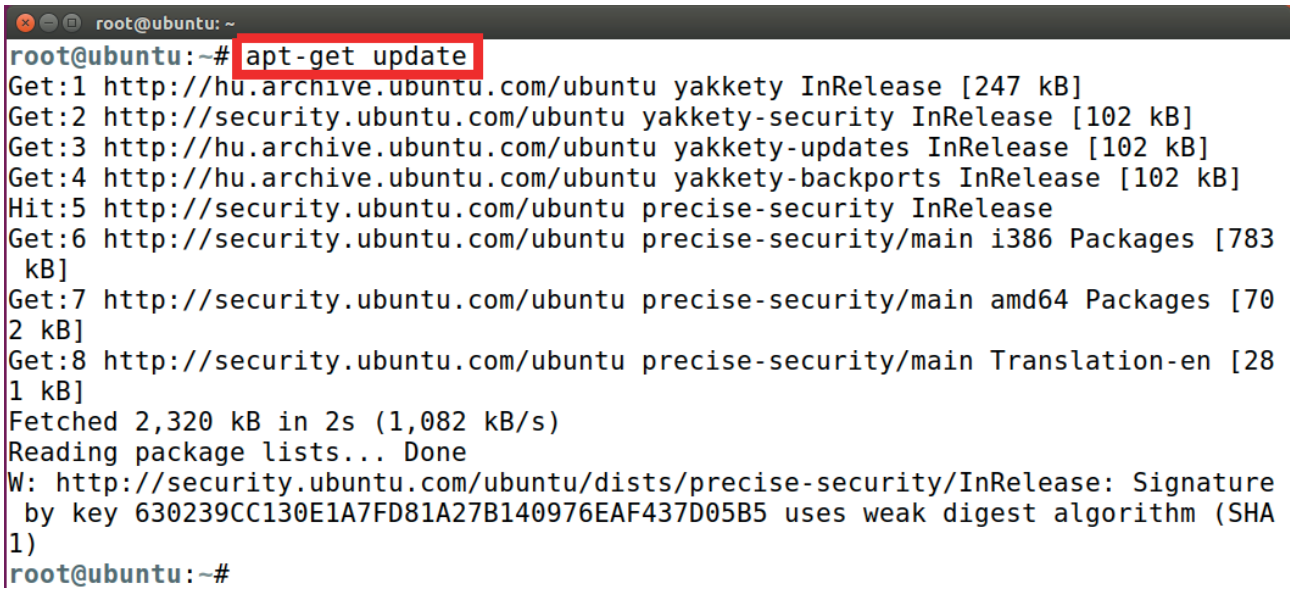
Adjuk hozzá a saját forensics laptopunk forráslistájához az ehhez a kernelhez tartozó letöltési címet: add-apt-repository „deb http://<megfelelő ubuntu archive>" az én esetemben: add-apt-repository „deb http://security.ubuntu.com/ubuntu precise-security main" Fontos, hogy a pontos kernelverzió kell, mert a különböző adatstruktúrák, melyek szükségesek, akár alverziónként is változhatnak.

19. ábra

Letöltési cím hozzáadása a forráslistához

Forrás: A szerző saját szerkesztése

Frissítsük a csomaglistát az apt-get update paranccsal.



20. ábra

A csomaglista frissítése az apt-get update paranccsal

Forrás: A szerző saját szerkesztése

Majd saját forensics laptopunkra letöltjük a vizsgálandó, a kernelverzióhoz való header fájlokat (ilyenkor szükséges a mobilinternet) például apt-get install linux-headers-<kernel verzió úgy, ahogy az előző parancs kiírta> az én példám esetében: apt-get install linux-headers-3.2.0-35-generic.

```
root@ubuntu: ~
root@ubuntu:~# apt-get install linux-headers-3.2.0-35-generic
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  linux-headers-3.2.0-35
The following NEW packages will be installed:
  linux-headers-3.2.0-35 linux-headers-3.2.0-35-generic
```

21. ábra

A vizsgálandó header fájlok letöltése

Forrás: A szerző saját szerkesztése

Bontsuk ki az alkalmazást!

```
root@ubuntu: ~/Downloads
root@ubuntu:~# cd Downloads/
root@ubuntu:~/Downloads# unzip ./LiME-master.zip
Archive:  ./LiME-master.zip
b4d13b820b5df2251c3ecd0dc5300d78411835a4
   creating: LiME-master/
  inflating: LiME-master/.gitignore
  inflating: LiME-master/LICENSE
  inflating: LiME-master/README.md
   creating: LiME-master/doc/
  inflating: LiME-master/doc/README.md
   creating: LiME-master/src/
  inflating: LiME-master/src/Makefile
  inflating: LiME-master/src/Makefile.sample
  inflating: LiME-master/src/disk.c
  inflating: LiME-master/src/lime.h
  inflating: LiME-master/src/main.c
  inflating: LiME-master/src/tcp.c
root@ubuntu:~/Downloads#
```

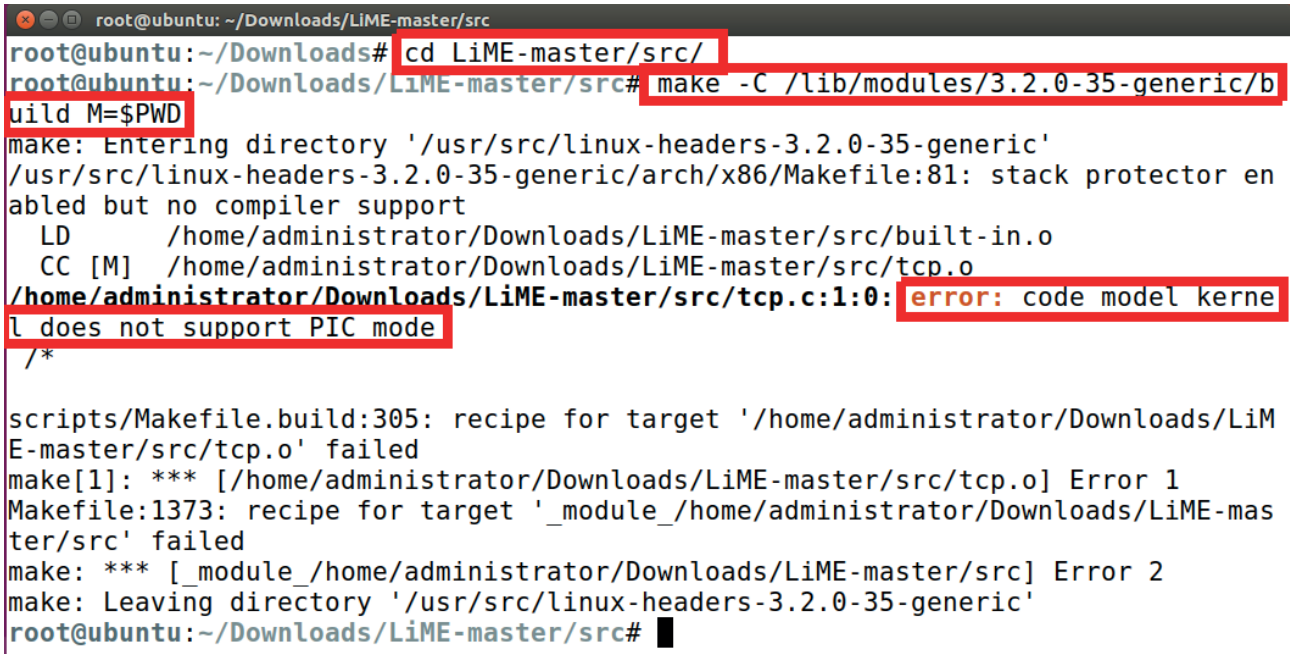
22. ábra

Az alkalmazás kibontása

Forrás: A szerző saját szerkesztése

Majd ehhez a kernelverzióhoz fordítjuk az alkalmazást. Lépjünk be a lime/src alkönyvtárba, és futtassuk a make -C /lib/modules/<kernel verzió>/build M=$PWD parancsot. Ekkor az én esetemben (linux 16.10-ről 12.10-re fordítok) egy csúnya hibaüzenet jelenik meg, melynek lényege a következő

sor: *„code model kernel does not support PIC mode”*. Ez azért történik, mert a gcc 5 verziótól kezdve alapértelmezetten Position Independent Code-ot (PIC) akar fordítani, viszont a régi kernel headerekben ez nem alapbeállítás.

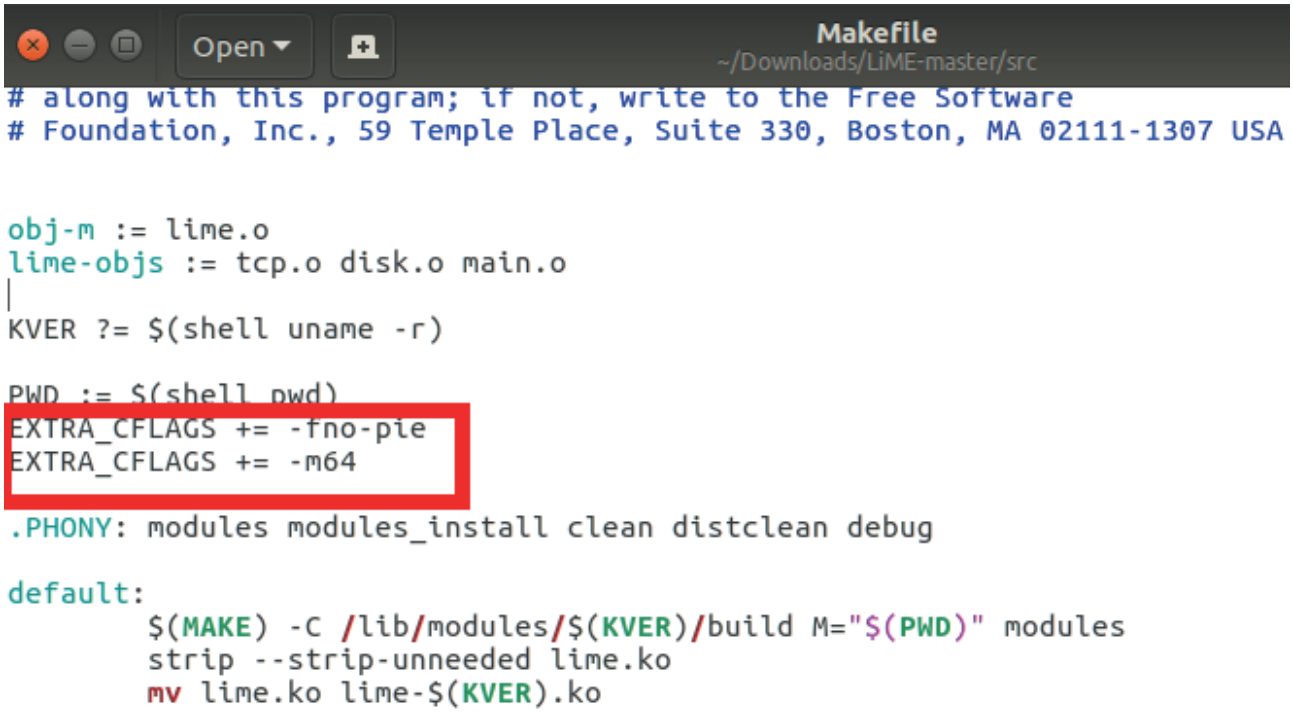


23. ábra

Lehetséges hibaüzenet az alkalmazás fordítása során

Forrás: A szerző saját szerkesztése

Hogy megoldjuk a problémát, adjuk hozzá az EXTRA_CFLAGS += -fno-pie sort lime Makefile-hoz. Ha 64 bites kódot akarunk fordítani, biztos, ami biztos alapon célszerű az EXTRA_CFLAGS += -m64 sort is.

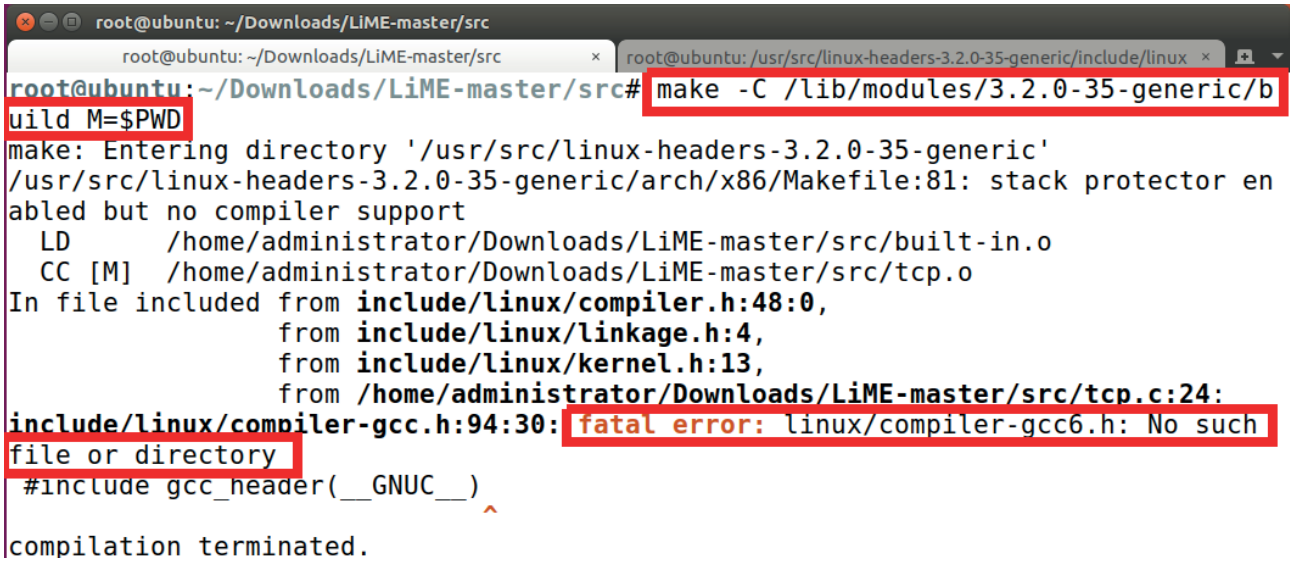


24. ábra

A felmerülő probléma megoldása az EXTRA_CFLAGS += -fno-pie sor hozzáadásával

Forrás: A szerző saját szerkesztése

Majd kíséreljük meg ismét a fordítást, ekkor egy másik hibaüzenetet kapunk. Ennek az az oka, hogy a gcc 6-os verzióval fordítunk, de a régi kernel esetében ez még nem is létezett. Tehát természetesen hiába keresi a gcc6 header fájljait a régi kernelforrásban.

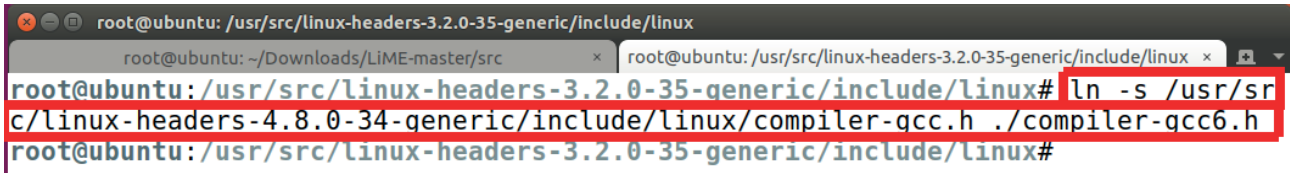


25. ábra

Hibaüzenet a fordítás megkísérlése során

Forrás: A szerző saját szerkesztése

Ezért készítsünk egy symbolic linket a saját kernelverziónk megfelelő fájljára!

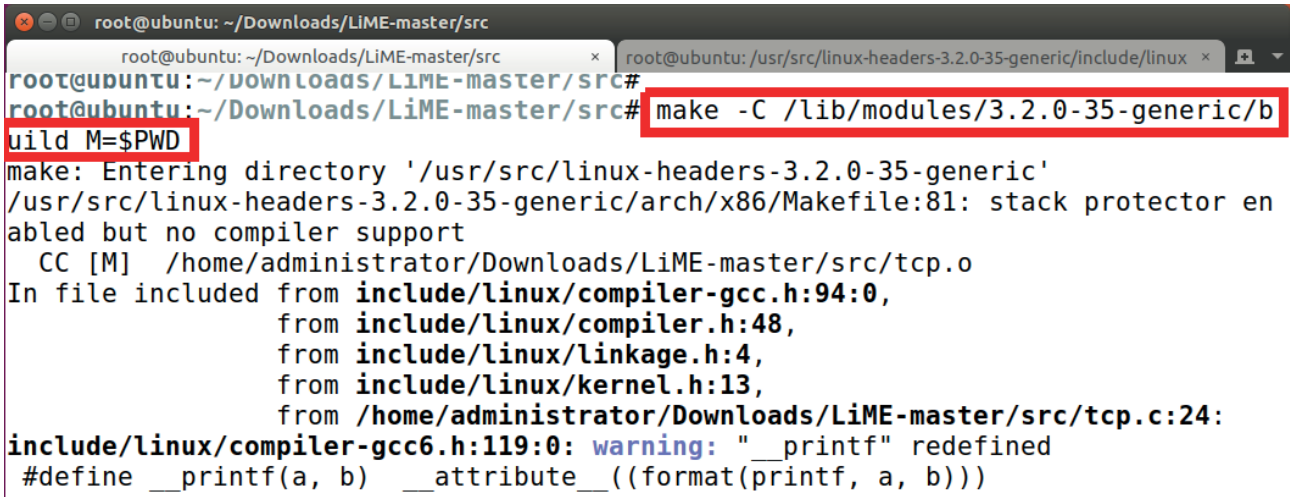


26. ábra

Symbolic link készítése

Forrás: A szerző saját szerkesztése

Majd fordítsuk le az alkalmazást, ekkor is sok figyelmeztetést kapunk, de már sikerülni fog.

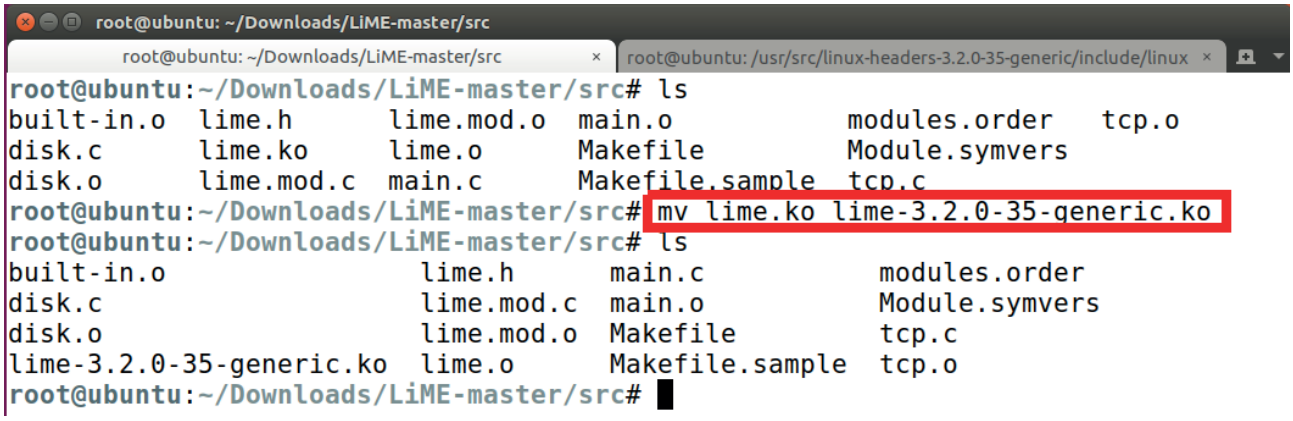


27. ábra

Az alkalmazás lefordítása

Forrás: A szerző saját szerkesztése

Javaslom, hogy nevezzük át az elkészült fájlt, hogy a neve tartalmazza a kernelverziót is, a későbbi könnyebb felhasználás érdekében.

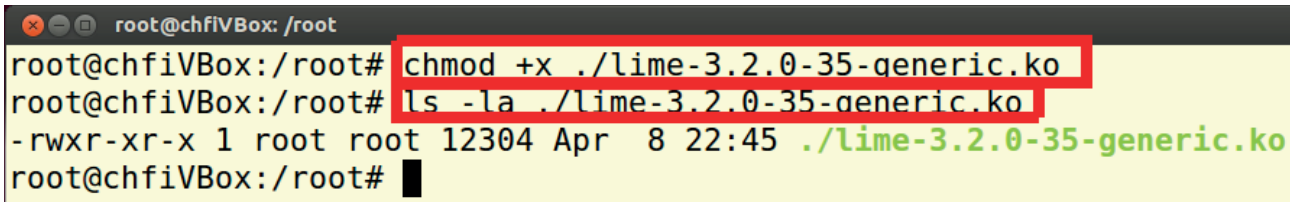


28. ábra

Az elkészült fájl átnevezése

Forrás: A szerző saját szerkesztése

Ezután az elkészült kernelmodult tegyük fel a pendrive-unkra, majd vigyük át a célgépre. Amennyiben szükséges, adjunk futtatási jogot a fájlhoz!

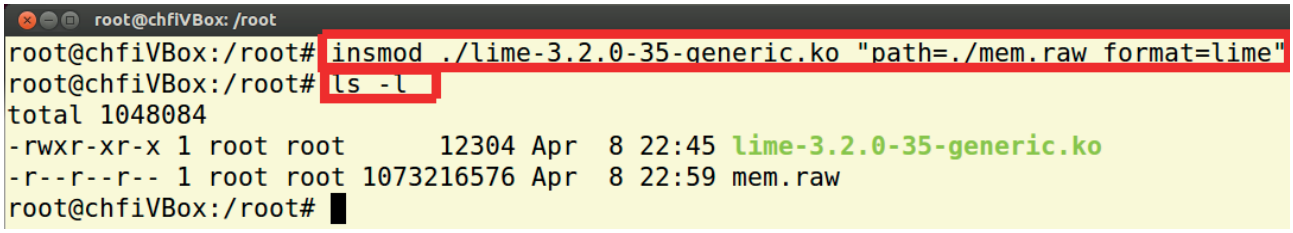


29. ábra

Futtatási jog hozzáadása az elkészült kernelmodulhoz

Forrás: A szerző saját szerkesztése

Ezután használhatjuk.



30. ábra

Az elkészült fájl használata

Forrás: A szerző saját szerkesztése

Mivel nem kapunk hash-t, ezért futtassunk egy hashkészítést is az elkészült memóriadumpra, majd a hashértéket vegyük jegyzőkönyvbe.

9.2.3. Másolat készítése az adathordozóról

Különböző alkalmazások más-más image fájl(oka)t készítenek:

- nyers, byte szintű másolat (raw);
- egyedi formátum, a metaadatok a fájlformátumban tárolva (proprietrary with embedded metadata);
- egyedi formátum, a metaadatok külön fájl(ok)ban tárolva (proprietrary with metadata in separate file[s])
- Nyers, byte szintű másolat, a metaadatok külön fájl(ok)ban tárolva (raw with hashes stored in separate files)

Mindegyik formátumnak megvan a maga előnye és hátránya.

- raw formátum
  - *Előnye:* egy fájl lesz az eredmény, ami könnyebben mozgatható. Könnyen kezelhető, az ilyen formátumban elkészített imaget rengeteg eszközzel fel tudjuk dolgozni, szinte bárhová be tudjuk csatolni.
  - *Hátránya:* nem készül alapból ellenőrző összeg, azt külön kell megcsinálni mind a forrásról, mind a másolatról, így jelentősen hosszabb az imagelés ideje.
  - Alkalmazás, amivel ilyet készíthetünk: dd
  - dd if=<source device> of=<output file> bs=<block size>

- Egyedi formátum, a metaadatok a fájlformátumban tárolva
  - *Előnye:* egy fájl lesz az eredmény, ami könnyebben mozgatható. Alapból készül ellenőrző összeg, esetleg hibaellenőrző kód is, így egy menetben megkapunk minden szükséges adatot, ezért gyorsabb. Az elterjedt, gyakori formátumok kezelésére (például EWF, AFF) vannak elkészített eszközök, amelyekkel csaknem olyan könnyen kezelhetők, mint egy raw image.
  - *Hátránya:* mivel egyedi formátum, nem biztos, hogy olyan könnyen tudjuk kezelni. Például ha megnyitjuk egy hexeditorral, mivel az adat és metaadat keveredik, az offseteket nehezebb követni.
  - Alkalmazás, amivel ilyet lehet készíteni: linen, ewfacquire
- Egyedi formátum, a metaadatok külön fájl(ok)ban tárolva
  - *Előnye:* alapból készül az ellenőrző összeg, esetleg hibaellenőrző kód is, így egy menetben megkapunk minden szükséges adatot, ezért gyorsabb. Mivel a metaadat és az image külön fájlban van, az imaget könnyebb használni. Ne keverjük össze a következő módszerrel, azért itt az egyedi formátum miatt konverziók igenis szükségesek.
  - *Hátránya:* mivel egyedi formátum, nem biztos, hogy olyan könnyen tudjuk kezelni. Több fájl van, melyeket együtt kell tartani.
- Nyers, byte szintű másolat, metaadatok külön fájl(ok)ban tárolva
  - *Előnye:* alapból készül ellenőrző összeg, esetleg hibaellenőrző kód is, így egy menetben megkapunk minden szükséges adatot, ezért gyorsabb. Mivel a metaadat, és az image külön fájlban van, az imaget könnyebb használni. A kapott image egy egyszerű raw image, ezért rengeteg eszközzel fel tudjuk dolgozni, szinte bárhová be tudjuk csatolni.
  - *Hátránya:* több fájl van, melyeket együtt kell tartani.
  - Alkalmazás, amivel lehet készíteni: dcfldd, d3dd
  - dcfldd if=<source device> of=<destination file> hash=<algorithm> hashwindow=<bytes> hashlog=<hash file> bs=<block size> split=<byte>

A legtöbb alkalmazás esetében a következő hashek közül választhatunk:

- *MD5:* nem ajánlott, de néhány régebbi alkalmazás csak ezt támogatja. Létezik ellene collision attack (tudunk olyan inputot generálni, ami ugyanazt a hash-t adja), ezért, ha egy alkalmazás csak ilyet támogat, mindenképpen készítsünk más hash-t is azonnal az elkészült outputról.
- *SHA1:* kivezetés alatt van, már ne használjuk. Az első sikeres támadást 2017 februárjában publikálták. Bár önmagában már egyik sem javasolt, MD5 és SHA1 együtt elfogadott.
- *SHA2 család (SHA256, SHA384, SHA512):* amennyiben lehetséges, ezeket használjuk, mert ez a legelterjedtebb, a legtöbb tool támogatja és CPU-kban általában szintén támogatott, tehát ennek leggyorsabb a használata is. A toolok nem biztos, hogy használják ezeket a kiterjesztett utasításkészleteit a CPU-nak.
- *Whirlpool:* a SHA2-vel közel megegyező szintű biztonságot nyújt, de kevésbé elterjedt, ezért toolokkal való kompatibilitás miatt nem annyira javasolt a használata.

Hashelés esetében erősen javasolt bizonyos adatmennyiségenként (hashwindow) is készíteni egy külön hash-t. Ez azért jó, mert ha netán sérülés történik a fájlban, akkor megállapítható, melyik résszel van probléma, és annak a kivételével a többi még felhasználható, nem kell a teljes bizonyítékot kidobni. Ez nem növeli meg az imagelés idejét észrevehetően, a mai CPU-k sokkal gyorsabbak, mint amennyi a disk sebesség, még SSD esetében is, és mivel sok CPU támogatja is például az SHA számítást utasításkészletből, így különösen gyors tud lenni, ha a toolok kihasználják a lehetőséget.

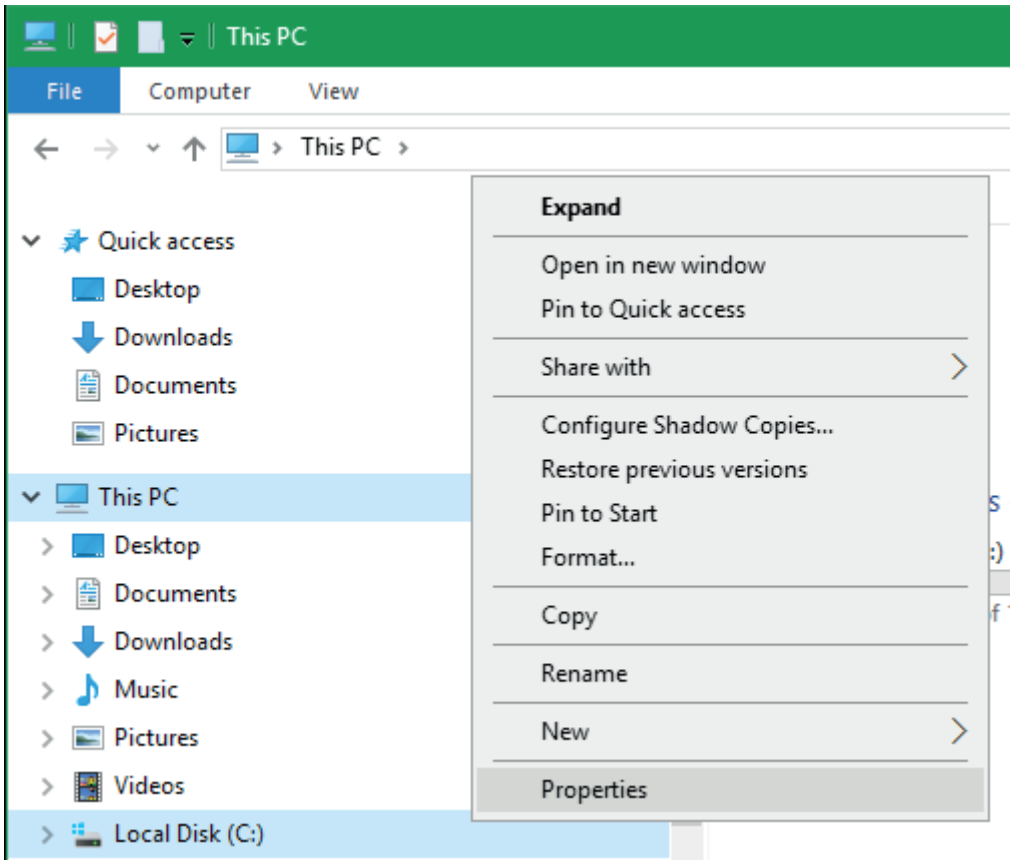
9.2.4. Disk Image készítése futó számítógépről

Ez a technika egyáltalán nem javasolt, de előfordulhat olyan eset, amikor nincs más választásunk, mert egy olyan kritikus rendszert kell vizsgálni, amit nem állíthatunk le.

9.2.4.1. Windows alapú gép

Windows alapú gépeknél használhatjuk a shadow copy-t, amennyiben támogatott. A módszer hátránya, hogy partícióra működik, nem egy egész diszkre.

Shadow copyt készítünk a rendszerről grafikusan: windows intéző \ jobb egér gomb a partíción \ properties:

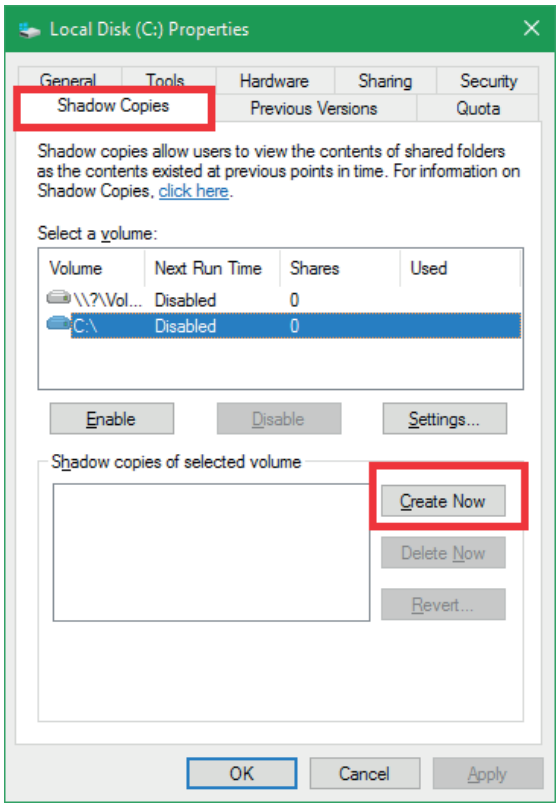


31. ábra

Shadow copy készítésének első lépései

Forrás: A szerző saját szerkesztése

Majd válasszuk a shadow copies fület, és kattintsunk a create now gombra:



32. ábra

Shadow copy készítése

Forrás: A szerző saját szerkesztése

Ezután parancssorból nézzük meg, mi lett az elkészült shadow copy neve, a vssadmin list shadows paranccsal:

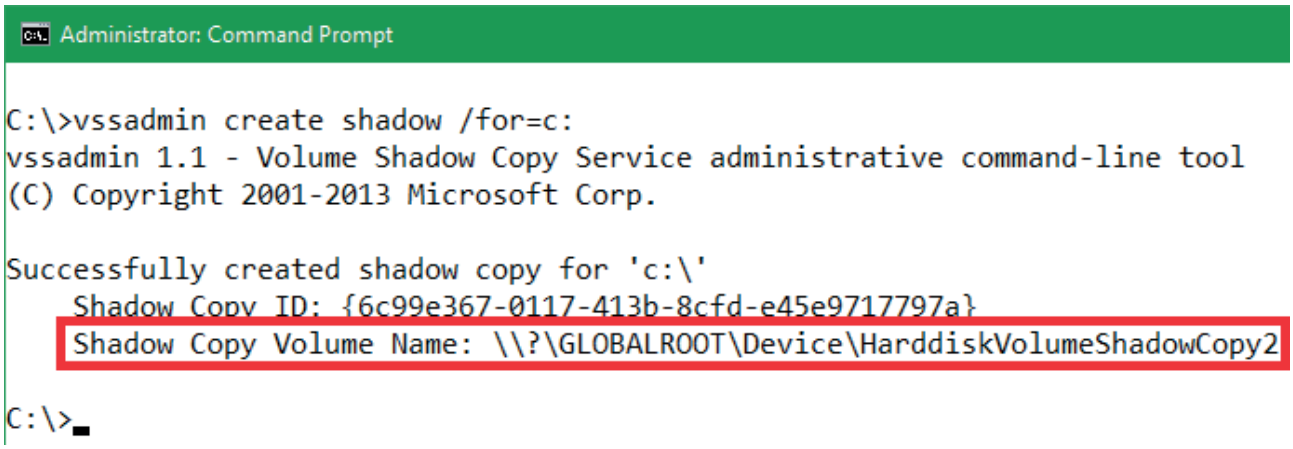
```
Administrator: Command Prompt
C:\>vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Contents of shadow copy set ID: {1c4d9dc2-73f6-4c0b-af3a-534fc6e3ecf8}
   Contained 1 shadow copies at creation time: 10/25/2016 2:14:11 AM
      Shadow Copy ID: {5959480d-58d4-4f02-99a0-f3d32eda19b0}
         Original Volume: (C:)\\?\Volume{74d289cd-0000-0000-0000-501f00000000}\
         Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
         Originating Machine: Attacker2k16
         Service Machine: Attacker2k16
         Provider: 'Microsoft Software Shadow Copy provider 1.0'
         Type: ClientAccessible
         Attributes: Persistent, Client-accessible, No auto release, No writers, Differential


C:\>
```

33. ábra

A shadow copy nevének ellenőrzése

Forrás: A szerző saját szerkesztése

Parancssorból is elkészíthetjük a shadow copy-t, a vssadmin create shadow /for=c: paranccsal.

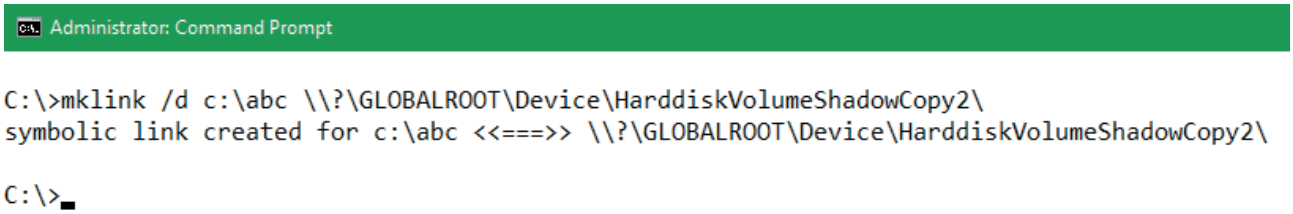


34. ábra

Shadow copy készítése parancssorból

Forrás: A szerző saját szerkesztése

Bármelyik esetben, amire szükségünk van, az a shadow copy volume name. Ezek után ezt a nevet használva létre tudunk hozni egy symbolic linket, az elkészült shadow copyra, így a fájlok már nem fogottak, és a teljes tartalmat tudjuk másolni. A symbolic link létrehozásához használjuk az mklink /d <link helye> <shadow copy volume name>\ parancsot. A \-t ne felejtsük el a név végén, különben nem fog működni (úgy tűnik, mintha működne, de üres alkönyvtárat kapunk eredményül).

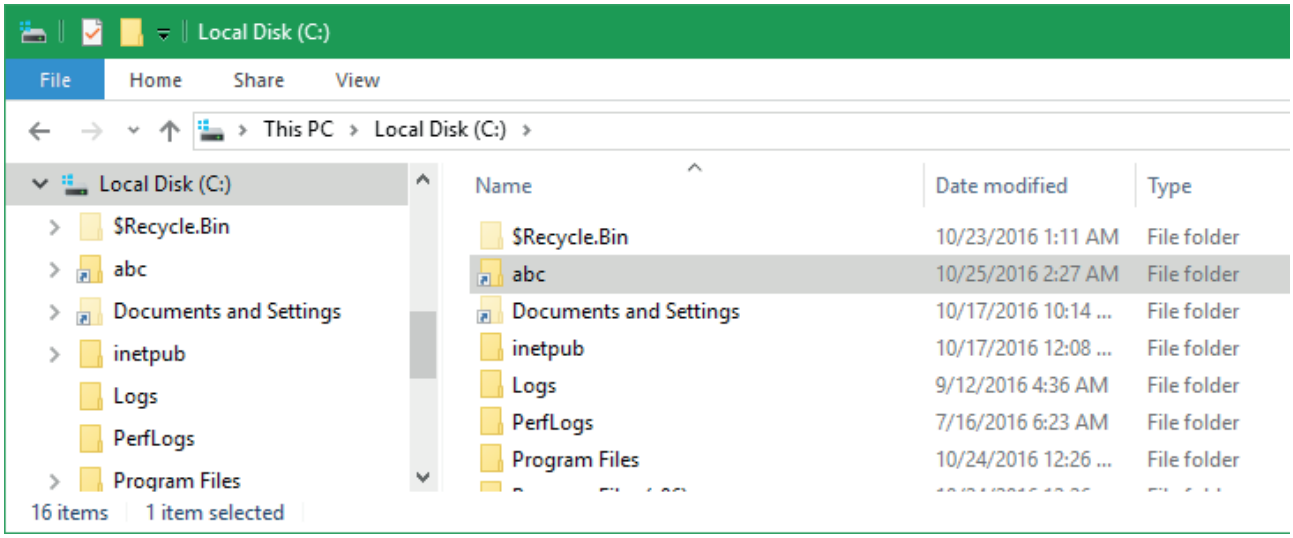


35. ábra

Symbolic link létrehozása

Forrás: A szerző saját szerkesztése

A kapott új symbolic link:



36. ábra

A kapott új symbolic link

Forrás: A szerző saját szerkesztése

Másik lehetőség shadow copy helyett, hogy használjuk a dcfldd alkalmazás windowsos változatát, és futtatjuk a következő parancsot:

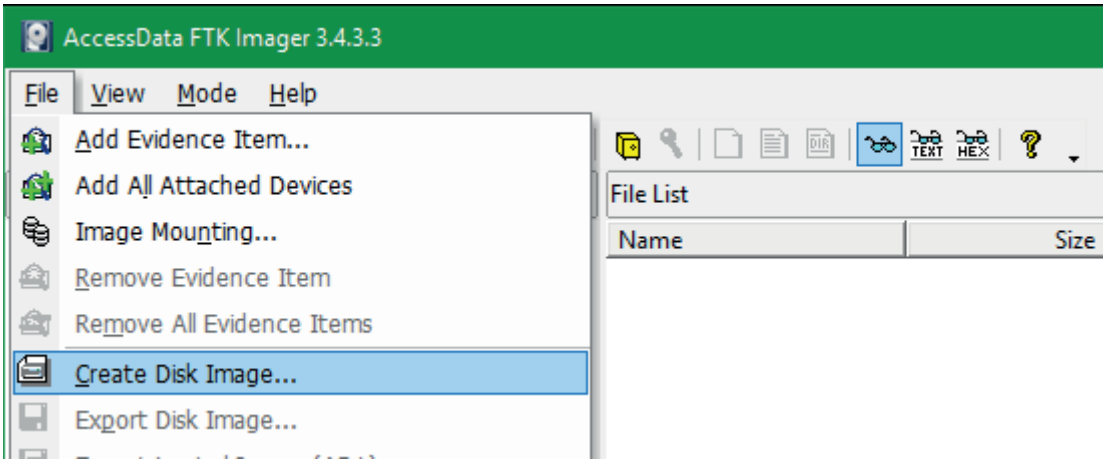
dcfldd -if=\\.\c: -of=x:\imgfile.img

Természetesen a hasheket is érdemes bekapcsolni, de én most csak azt akartam megmutatni, hogyan adjuk meg a forrást ebben az esetben; a \\.\ előtétet kell alkalmazni.

9.2.4.2. Másolat készítése az FTK imager alkalmazással

Az FTK, a „The Forensic Toolkit” nevű elterjedt alkalmazás neve, aminek van egy ingyenesen letölthető és használható imager része (a legtöbb fizetős alkalmazásra igaz, hogy a hozzá tartozó image készítő ingyenesen elérhető, hiszen a gyártónak is érdeke, hogy minél többen az ő formátumában készítse az image-t). A tool képes többek között disk és memória imagelésre is. Alapértelmezés szerint sajnos telepíteni kell, de ha saját gépre telepítjük, majd a binárisokat lemásoljuk, működni szokott pendrive-ról is. Azonban itt azért előjöhetnek hiányzó dll, dependenciák,vagy egyéb gondok, ezért célszerű mellette mindig tartani alternatív megoldást. A bizonyítékgépre ne telepítsük. Előnye, hogy kényelmes, könnyen használható grafikus alkalmazás. Mivel egy elterjedt fizetős termék része, rendszeres és megbízható a frissítése, az új operációs rendszerek követése.

Disk image készítéséhez indítsuk el az alkalmazást, majd válasszuk a File / Create Disk Image... menüpontot.

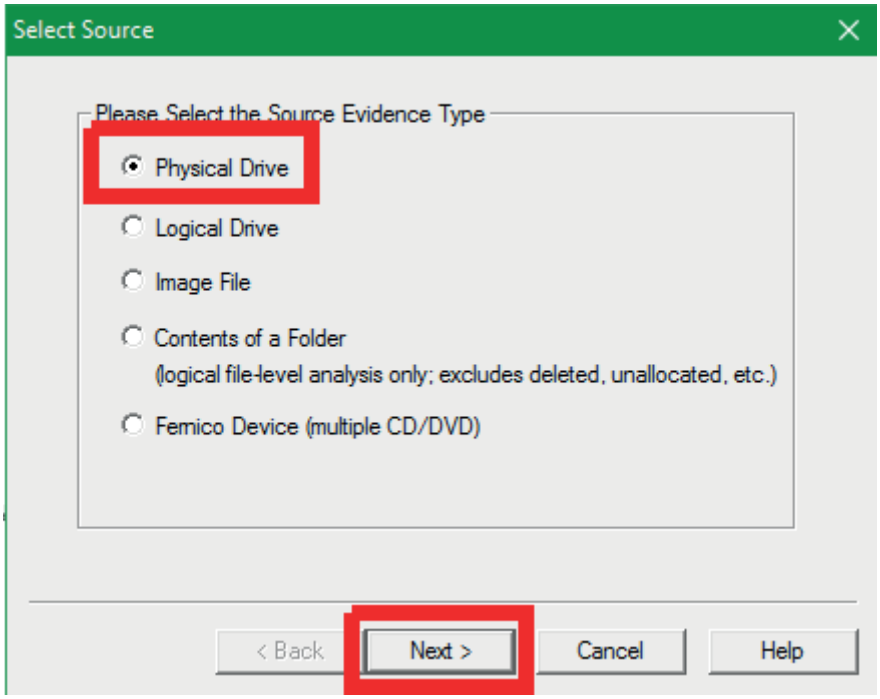


37. ábra

Az alkalmazás indítása Disk image készítéséhez

Forrás: A szerző saját szerkesztése

Ki lehet választani, mit imageljünk, a teljes fizikai diszket (általában ez javasolt) vagy logikai diszket, alkönyvtárat, másik image fájlt.

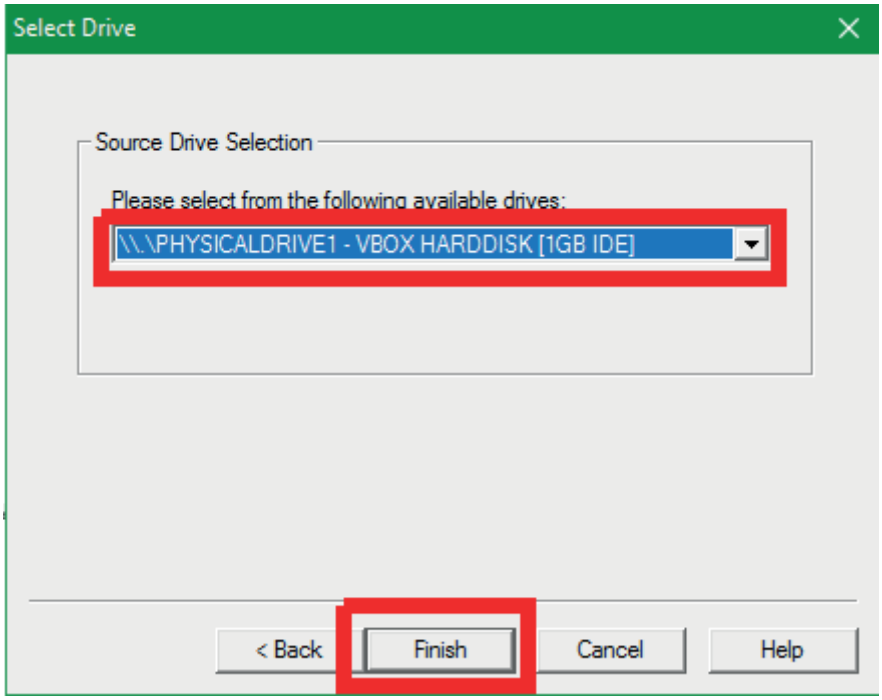


38. ábra

Annak az elemnek a kiválasztása, amelyet imagelni szeretnénk

Forrás: A szerző saját szerkesztése

Válasszuk ki a forrást:

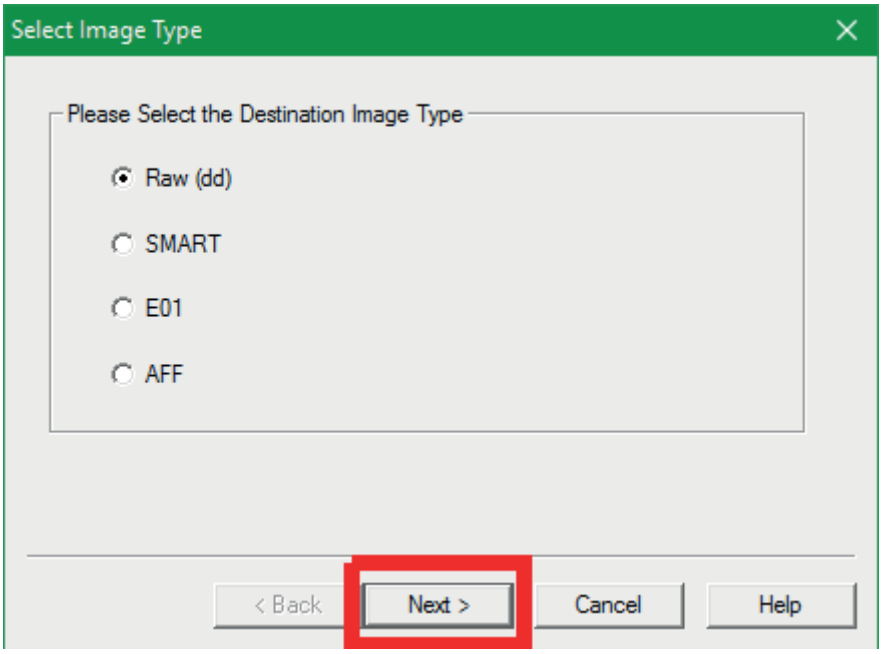


39. ábra

A forrás kiválasztása

Forrás: A szerző saját szerkesztése

Ezután adjuk meg a készítendő image formátumát. Ismeri természetesen a raw imaget, illetve az elterjedtebb forensics formátumokat is.

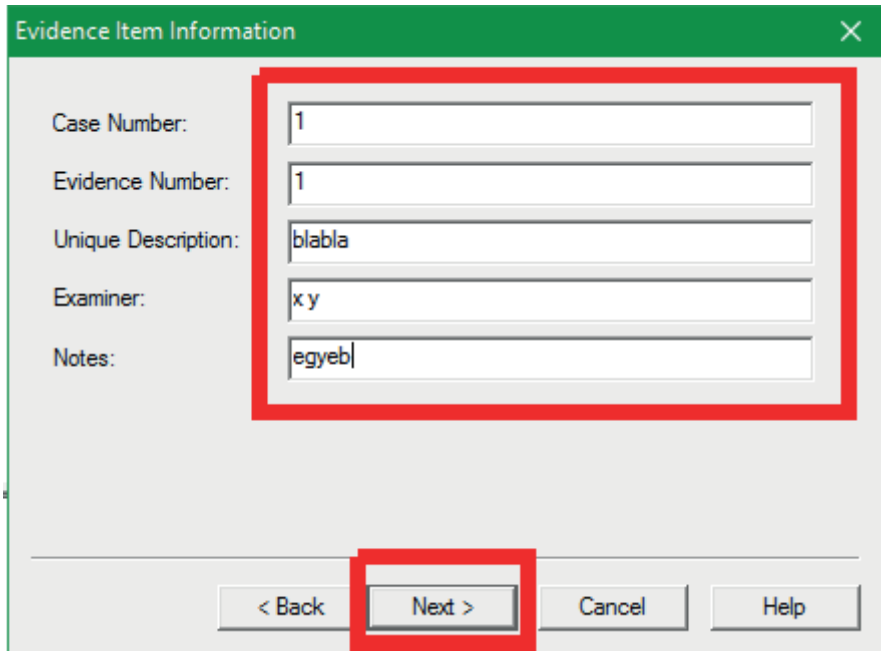


40. ábra

A készítendő image formátumának kiválasztása

Forrás: A szerző saját szerkesztése

Adjuk meg az ügyszámot, bizonyíték számot, leírást, imagelést végző személy nevét, és egyéb megjegyzéseinket, ha vannak.

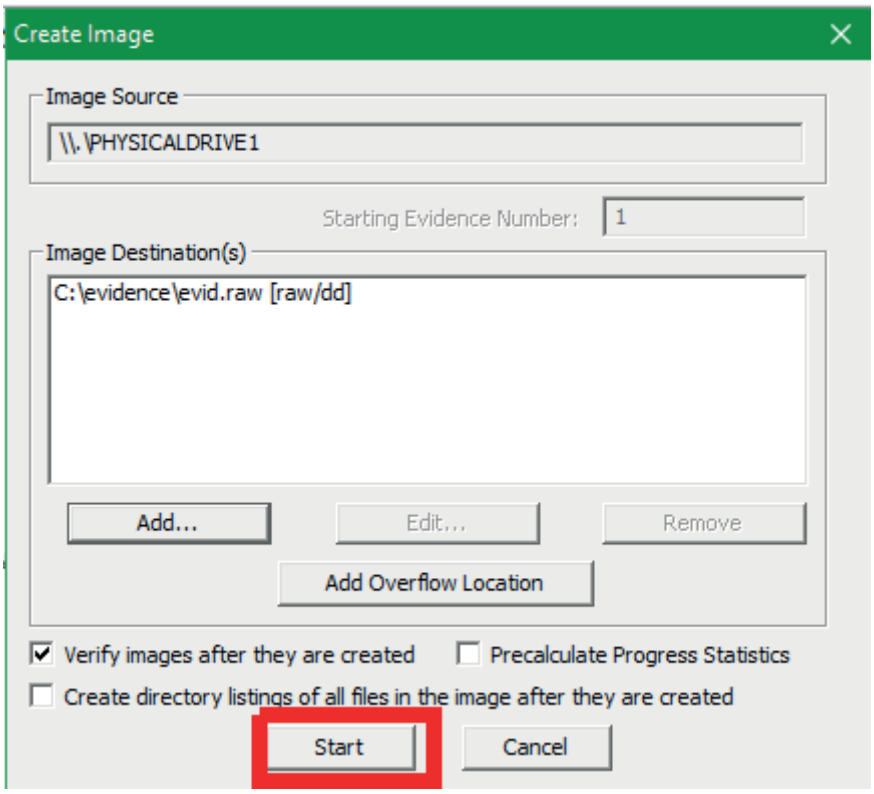


41. ábra

Az imagelés információinak megadása

Forrás: A szerző saját szerkesztése

Kapunk egy összefoglaló képet. Amennyiben van lehetőségünk, készítsünk listát az imageben lévő fájlokról, majd kattintsunk a Start gombra.

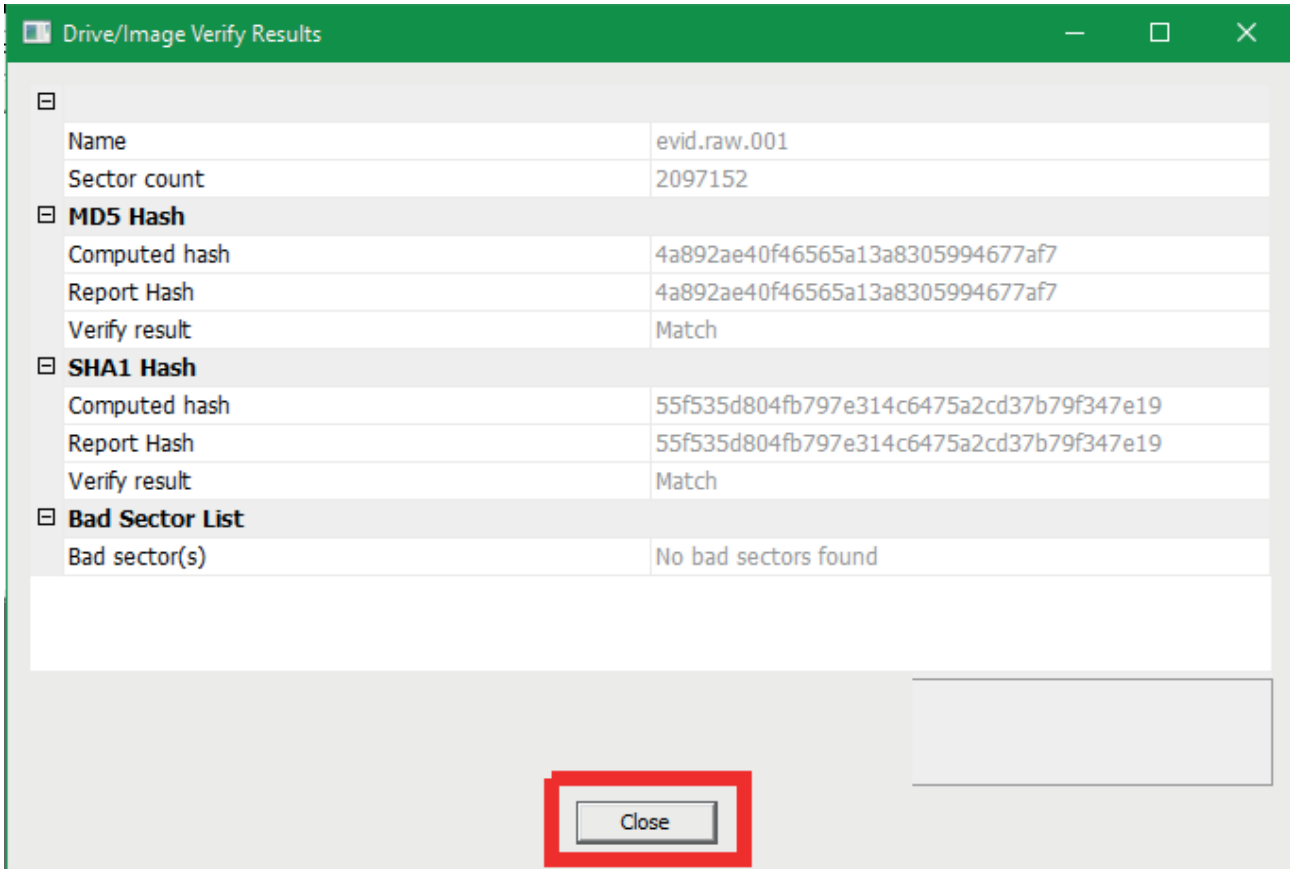


42. ábra

Összefoglaló kép a folyamatról

Forrás: A szerző saját szerkesztése

Az imagelés végeztével kapunk egy ablakot, ami tartalmazza a hashértékeket. Ezeket vegyük jegyzőkönyvbe.



43. ábra

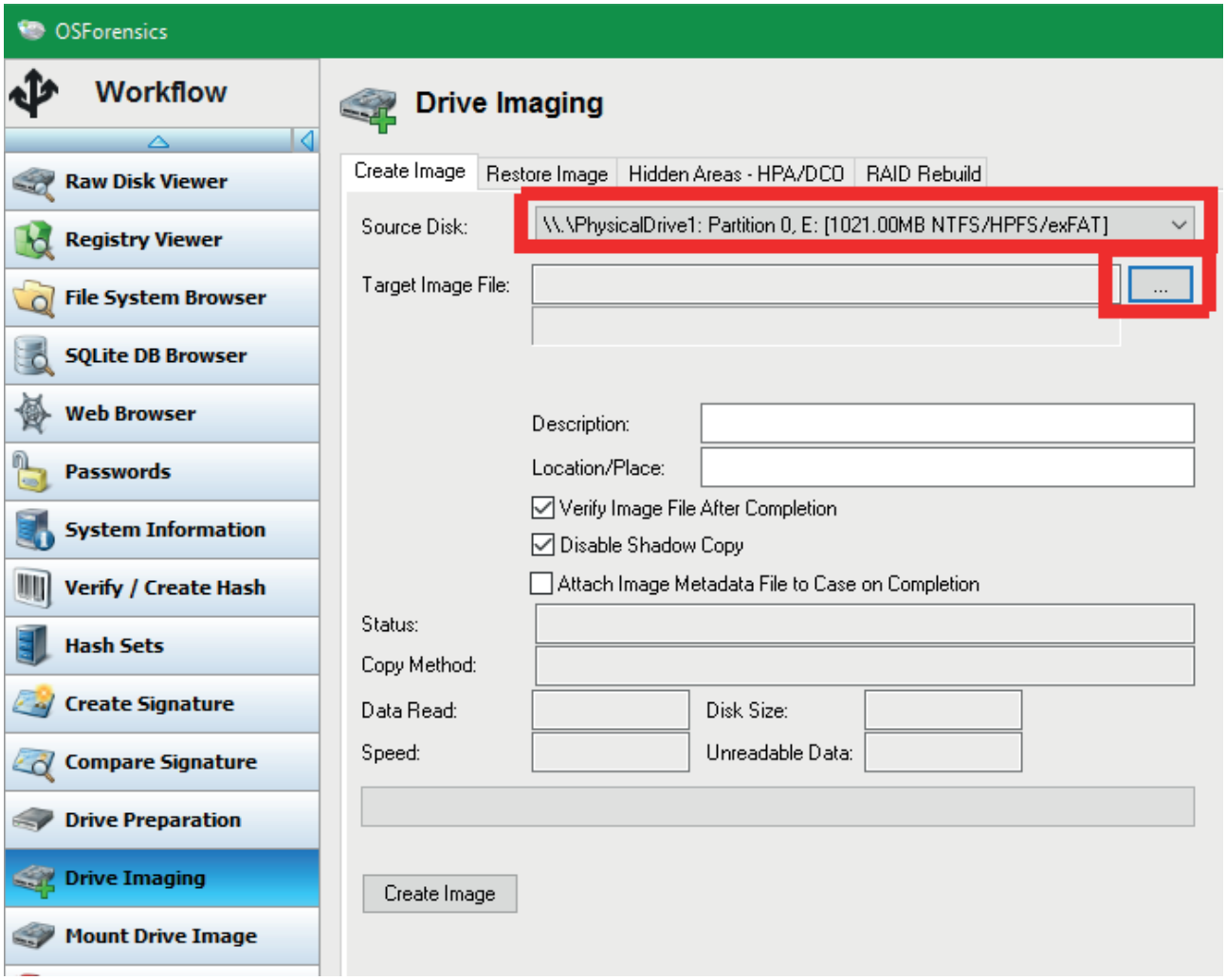
A hashértékeket tartalmazó ablak

Forrás: A szerző saját szerkesztése

9.2.4.3. Másolat készítése az OSF alkalmazással

Az OSF az OS Forensics nevű ingyenes forensics analizáló program futtatható állománya. Csak úgy, mint az előző FTK imager, ez is alapvetően egy telepítést igénylő alkalmazás, de ha saját gépre telepítjük, van egy copy to usb menüpontja, ami a binárisokat lemásolja egy pendrive-ra. Ez nagy valószínűséggel megfelelően fog futni a vizsgálandó gépen. Szintén képes többek között disk, és memória image készítésére, de azonkívül ez egy teljes analizáló környezet is. Amennyiben egy egyszerűbb, all in one grafikus alkalmazást szeretnénk használni a parancssori eszközök helyett, akkor jó választás lehet számunkra.

Bal oldalt keressük meg a drive image lehetőséget, majd válasszuk ki a forrásdisket. Ezután kattintsunk a target image file: sor mellett a „...” ikonra.

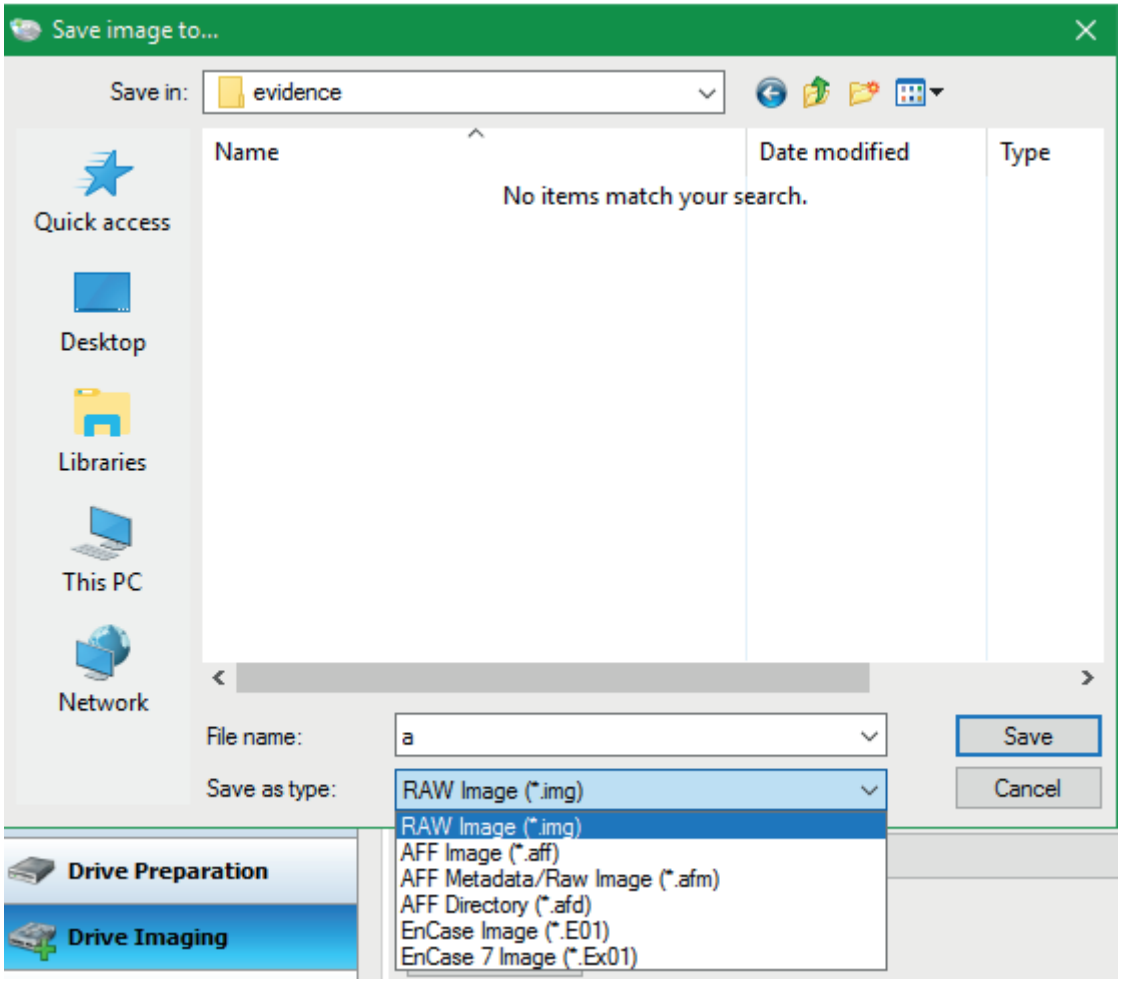


44. ábra

A forrásdisk kiválasztása

Forrás: A szerző saját szerkesztése

Adjuk meg a célfájl nevét, és válasszuk ki a formátumot. Szintén minden elterjedtebb formátumot ismer. Miután ezeket beállítottuk, kattintsunk a save gombra.

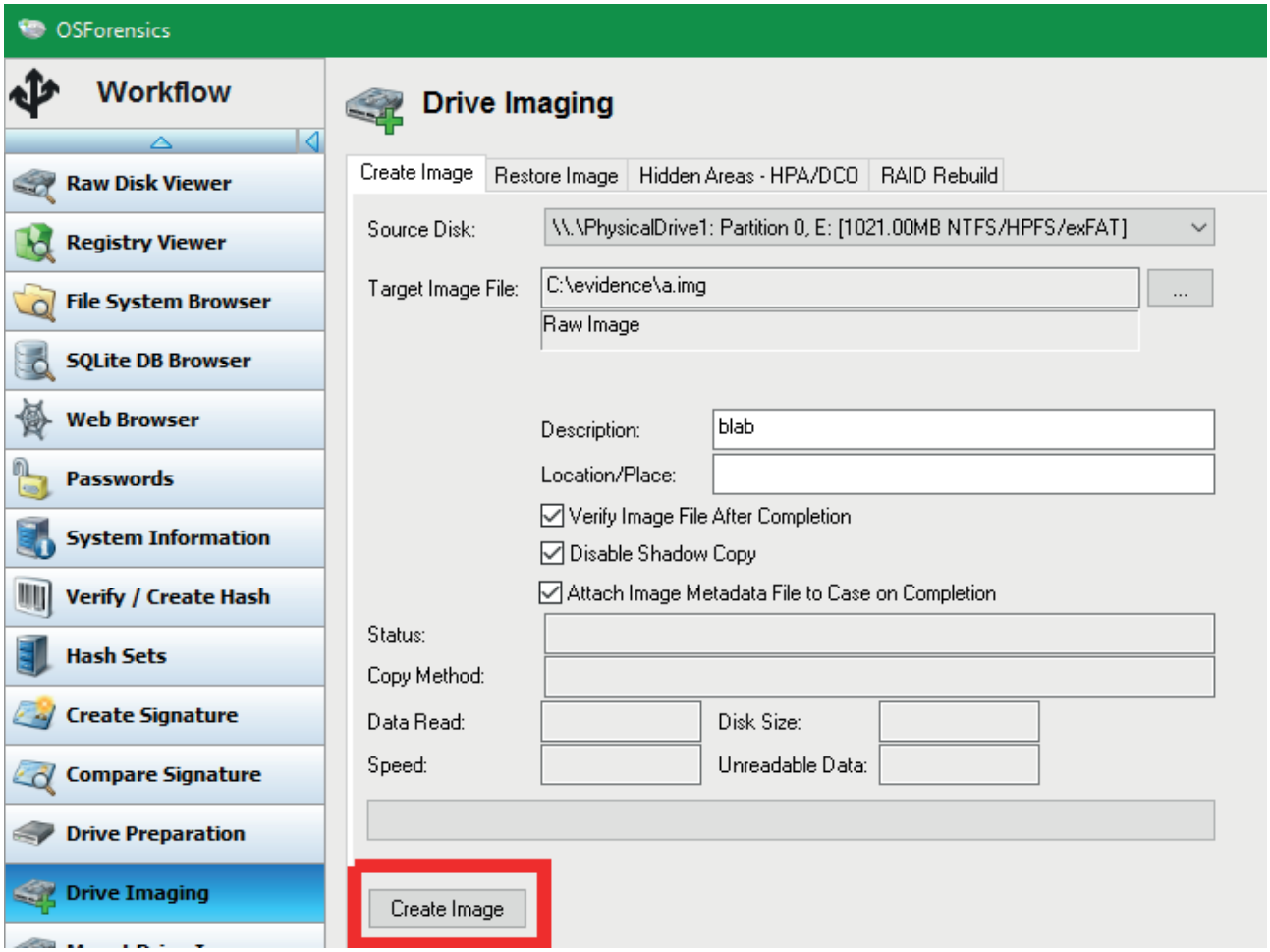


45. ábra

A célfájl nevének és formátumának megadása

Forrás: A szerző saját szerkesztése

Adjuk meg az egyéb információkat is. Ha van rá lehetőség, készítsünk metadata infofájlt is, majd kattintsunk a Create image gombra.

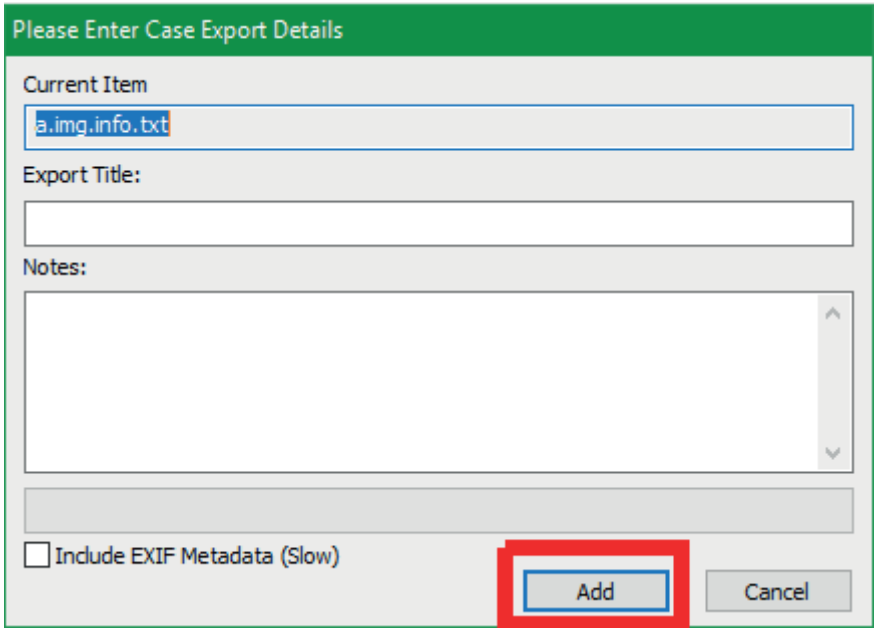


46. ábra

Egyéb információk megadása

Forrás: A szerző saját szerkesztése

Ha kértünk metadata információkat, kapunk egy ablakot, ahol megadhatjuk a fájl nevét, és az egyéb jegyzeteket is beleírhatjuk. Amennyiben van rá lehetőség, az exif adatokat dolgozzuk fel most, hogy a későbbiekben ne kelljen, de amennyiben több lefoglalásra váró adathordozó is van, inkább azokra fordítsunk nagyobb hangsúlyt, mert ez később is elvégezhető.



47. ábra

Metadata információk megadása

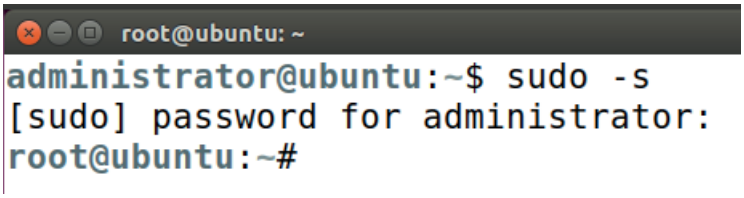
Forrás: A szerző saját szerkesztése

9.2.5. Disk image készítése kikapcsolt számítógépről

Image készítésére ez a javasolt módszer, ha csak lehet, ezt alkalmazzuk. Ebben az esetben nincs jelentősége, hogy a forrásgép, amit imagelni szeretnénk, milyen operációs rendszert használ.

Amennyiben rendelkezünk másoló eszközzel, az eljárás elég egyszerű, csatlakoztatjuk a forrásmerevlemezt a forrásoldalra, a célmerevlemezt a céloldalra, és a menüből elindítjuk a másolást. A folyamat végén kapott ellenőrző összegeket jegyzőkönyvbe vesszük.

Amennyiben nem rendelkezünk másoló eszközzel, használjuk a forensics laptopot. Lépjünk be, majd nyissunk egy terminálablakot. A legtöbb alkalmazás, amit használunk, alacsony szintű hozzáférést igényel, ezért váltsunk root jogra, legtöbb debian alapú rendszernél sudo -s, vagy sudo bash, vagy sudo sh, vagy hasonló paranccsal, majd adjuk meg a jelszavunkat:



48. ábra

Terminálablak megnyitása

Forrás: A szerző saját szerkesztése

Listázzuk ki, milyen adathordozók vannak csatlakoztatva. Ezt az fdisk -l, vagy az lsblk paranccsal tudjuk megtenni.

```
Disk /dev/mapper/ubuntu--vg-swap_1: 4 GiB, 4294967296 bytes, 8388608 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
root@ubuntu:~#
```

49. ábra

A csatlakoztatott adathordozók kilistázása

Forrás: A szerző saját szerkesztése

Ezután csatlakoztatjuk a forrást egy írásblokkolóhoz, majd a forenics laptophoz. Ezt követően ismét kérdezzük le az fdisk -l, vagy az lsblk paranccsal, milyen adathordozók vannak, és keressük meg az új eszköz azonosítóját. Nekem sdb. Amennyiben partíciók is vannak, azok sdb1, sdb2 stb. névvel jelennek meg. Tipikusan, hacsak valami nagyon erős ellentétes indok nincs, például raid, amit nem akarunk ismét összerakni (bár akkor is célszerű a partíciókon kívül a diskeket is imagelni egy külön lépésként, még ha ez duplamunka is), akkor az egész diske(ke)t imageljük, ne csak külön-külön az egyes partíciókat.

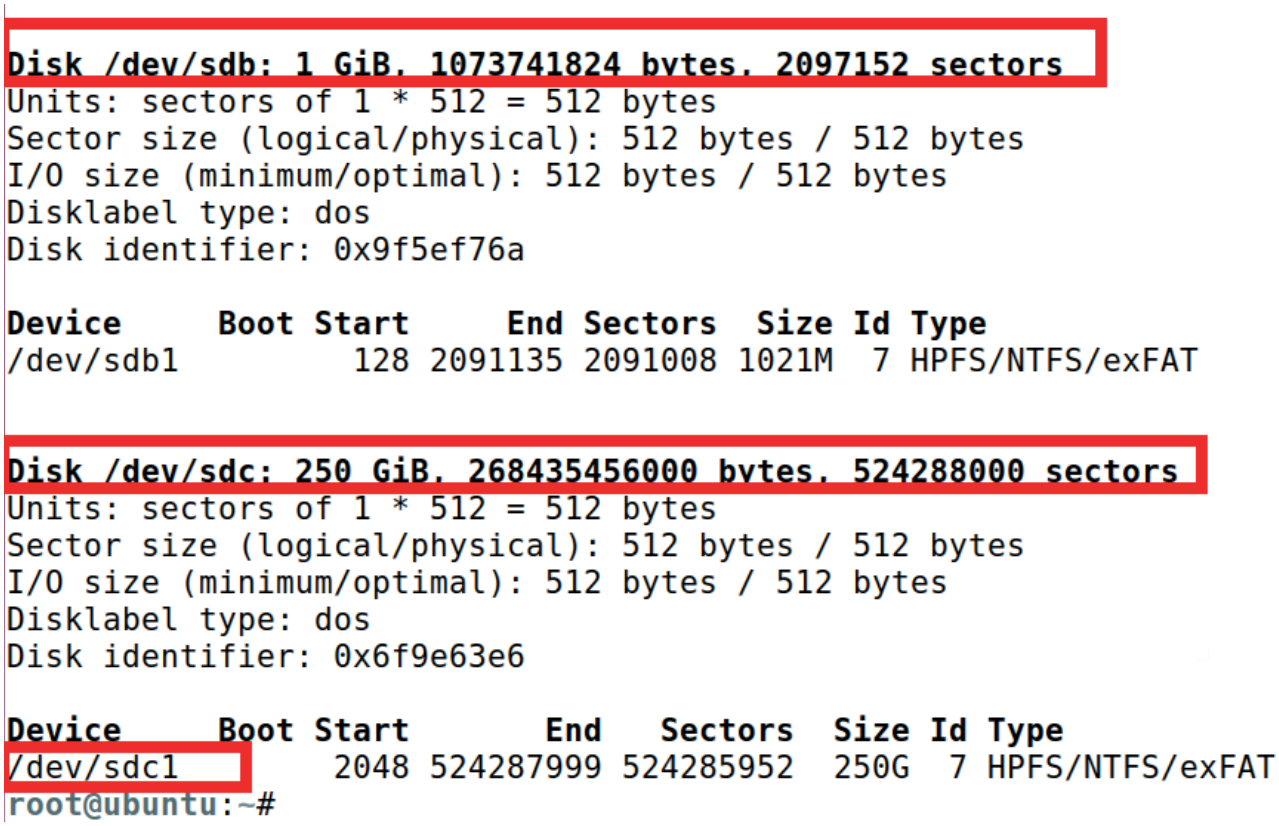
```
Disk /dev/sdb: 1 GiB, 1073741824 bytes, 2097152 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x9f5ef76a

Device     Boot Start     End Sectors  Size Id Type
/dev/sdb1        128 2091135 2091008 1021M  7 HPFS/NTFS/exFAT
root@ubuntu:~#
```

50. ábra

Az imagelés

Forrás: A szerző saját szerkesztése

Csatlakoztassuk a céleszközt is, szintén kérdezzük le, milyen eszköznevet kapott, nekem sdc. Míg az előbb a teljes diszket akartuk használni, addig a céleszköznél tipikusan a fiájlrendszerre írunk, tehát nekem a rajta lévő sdc1 partíció kell majd.

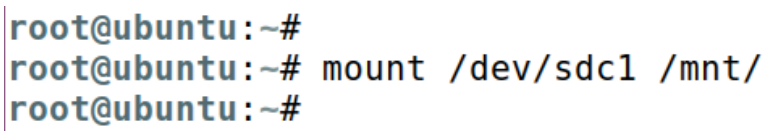


51. ábra

Az eszköznév lekérdezése

Forrás: A szerző saját szerkesztése

Mountoljuk be a céleszközt, hogy legyen hová írni:



52. ábra

A céleszköz mountolása

Forrás: A szerző saját szerkesztése

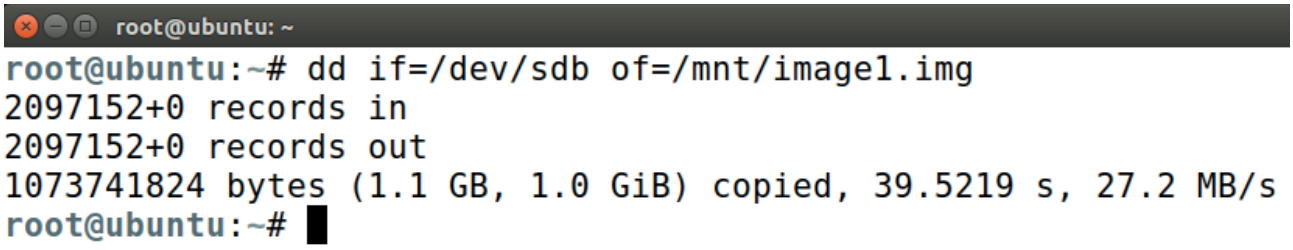
Ezután elindítjuk a másolatkészítést. Néhány elterjedt és már korábban megemlített alkalmazással történő imagelés parancsait mutatjuk be, de ezeken kívül természetesen egyéb megfelelő paraméterekkel rendelkező alkalmazások szintén használhatók.

9.2.5.1. Másolatkészítés dd paranccsal

A dd parancs minden linuxos rendszeren megtalálható, segítségével raw imagemásolatot készíthetünk egyszerűen.

A legfontosabb kapcsolók a következők:

- másolás forrása if=. Például: if=/dev/sdb
- másolás célja of=. Például: of=/mnt/image

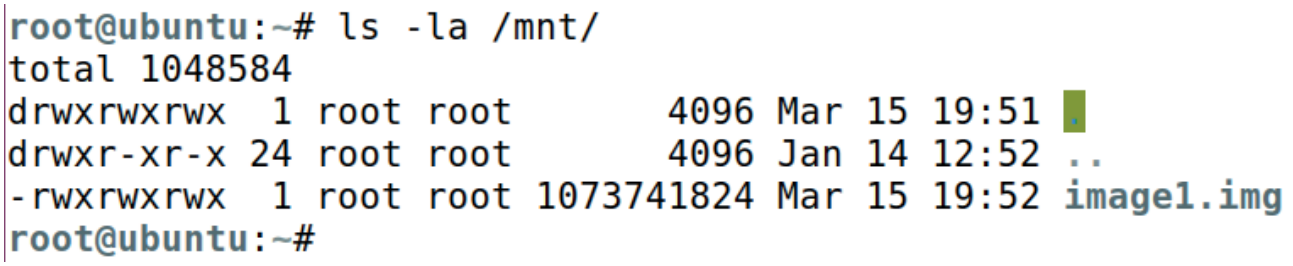


53. ábra

Raw imagemásolat készítése

Forrás: A szerző saját szerkesztése

Ha elkészült, ellenőrizzük a kapott fájlokat!

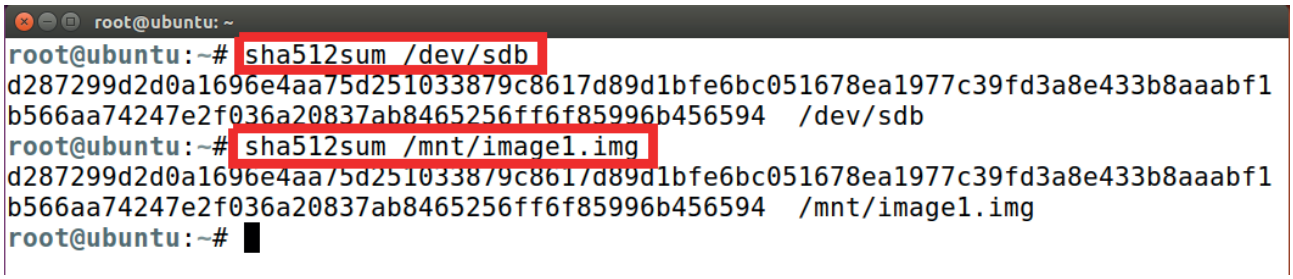


54. ábra

A kapott fájlok ellenőrzése

Forrás: A szerző saját szerkesztése

Sajnos ebben az esetben nem kapunk ellenőrző összeget azonnal, egy külön lépésben le kell futtatni egy hashelő alkalmazást (például sha1sum, sha256sum, sha384sum, sha512sum) mind a forrás-, mind a célfájlra.



55. ábra

Hashelő alkalmazás futtatása

Forrás: A szerző saját szerkesztése

A hashértéket mindenképpen foglaljuk bele a házkutatási jegyzőkönyvbe is. Erre azért van szükség, mert a hash csak a véletlen módosulás ellen véd, a szándékosság ellen nem. Tehát egy rosszindulatú elemző visszaállíthatja a raw imaget, bizonyítékot helyez el benne, vagy távolít el, majd erről az új változatról készít imaget, és az eredetit erre kicseréli. Az ilyen beavatkozások ellen véd a több tanú által aláírt, helyszínen készült jegyzőkönyv.

9.2.5.2. Másolatkészítés a dcfldd alkalmazással

A forensics laptopra még a munka megkezdése előtt, az előkészületek során telepítsük az alkalmazást, az apt-get install dcfldd paranccsal.

```
root@ubuntu:~# dcfldd
The program 'dcfldd' is currently not installed. You can install it by typing:
apt install dcfldd
root@ubuntu:~#
```

```
root@ubuntu:~# apt-get install dcfldd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  dcfldd
0 upgraded, 1 newly installed, 0 to remove and 146 not upgraded.
Need to get 38.3 kB of archives.
After this operation, 128 kB of additional disk space will be used.
Get:1 http://hu.archive.ubuntu.com/ubuntu yakkety/universe amd64 dcfldd amd64
1.3.4.1-9 [38.3 kB]
Fetched 38.3 kB in 0s (316 kB/s)
Selecting previously unselected package dcfldd.
(Reading database ... 209351 files and directories currently installed.)
Preparing to unpack .../dcfldd_1.3.4.1-9_amd64.deb ...
Unpacking dcfldd (1.3.4.1-9) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up dcfldd (1.3.4.1-9) ...
root@ubuntu:~#
```

56. ábra

Az alkalmazás telepítése

Forrás: A szerző saját szerkesztése

Indítsuk el a másolást, a következő kapcsolók fontosak:

- másolás forrása if=, például: if=/dev/sdb;
- másolás célja of=, például: of=/mnt/image;
- számított hashtípus hash=, például: hash=sha512;
- mekkora adatblokkonként számoljon hash-t hashwindow=, például: hashwindow=64k;
- melyik fájlba írja a számított hashértékeket hashlog= például: hashlog=/mnt/image.hash;
- mekkora egységekre törje a kapott eredményfájlt split= például: split=512M.

```
root@ubuntu:~# dcfldd if=/dev/sdb of=/mnt/imag1.img hash=sha512 hashwindow=64k
 hashlog=/mnt/imag1.hash
7168 blocks (224Mb) written.
```

57. ábra

A másolás elindítása

Forrás: A szerző saját szerkesztése

A következő eredményfájlokat kapjuk:

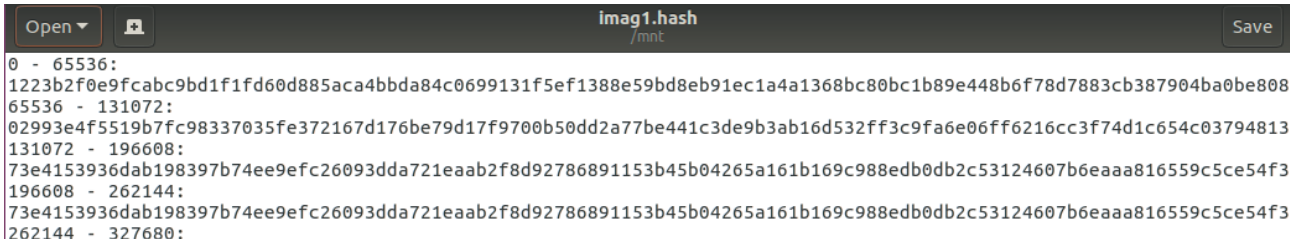
```
root@ubuntu:~# ls -la /mnt/
total 1051016
drwxrwxrwx  1 root root       4096 Mar 15 19:42 .
drwxr-xr-x 24 root root       4096 Jan 14 12:52 ..
-rwxrwxrwx  1 root root    2489370 Mar 15 19:42 imag1.hash
-rwxrwxrwx  1 root root 1073741824 Mar 15 19:42 imag1.img
root@ubuntu:~#
```

58. ábra

A kapott eredményfájlok

Forrás: A szerző saját szerkesztése

A kapott hashfájlt megnyitásával látjuk a blokkonként kapott hasheket:

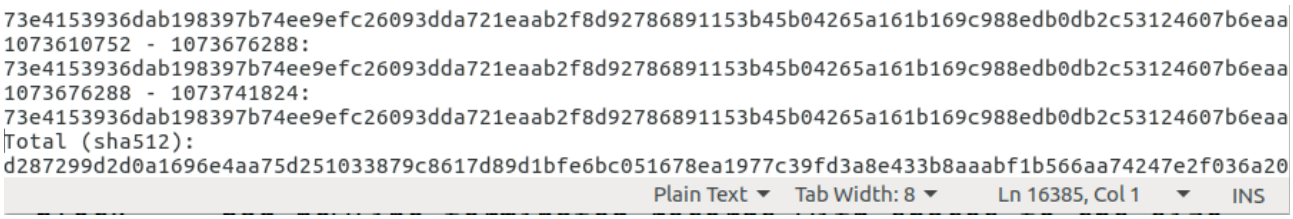


59. ábra

A kapott hashek blokkonként

Forrás: A szerző saját szerkesztése

A file legvégén megkapjuk a total hashértéket is.



60. ábra

A totál hashérték

Forrás: A szerző saját szerkesztése

Az összes hash nyilván nagyon sok, de a total hash értéket mindenképpen foglaljuk bele a házkutatási jegyzőkönyvbe is. Ahogy az előző példában, most is azért van szükség, mert a hash csak a véletlen módosulás ellen véd, a szándékosság ellen nem. Tehát egy rosszindulatú elemző visszaállíthatja a raw imaget, bizonyítékot helyez el benne vagy távolít el, majd erről az új változatról készít imaget, és az eredetit erre kicseréli. Az ilyen beavatkozások ellen véd a több tanú által aláírt, helyszínen készült jegyzőkönyv.

Ezután a hashfájlról készítsünk egy hash-t, amit szintén jegyzőkönyvbe kell venni. Ha sérülés történik az adatokban, szükségünk lesz a bennük lévő hashekre, de mindet leírni jegyzőkönyvbe kivitelezhetetlen. Ezzel tudjuk bizonyítani, hogy az a hashfájl tényleg ugyanaz, és más blokkok nem módosultak.

9.2.5.3. Másolatkészítés ewfacquire alkalmazással

A forensics laptopra még a munka megkezdése előtt, az előkészületek során telepítsük az alkalmazást, az apt-get install ewf-tools paranccsal.

```
root@ubuntu: ~
root@ubuntu:~# ewfacquire
The program 'ewfacquire' is currently not installed. You can install it by typ
ing:
apt install ewf-tools
root@ubuntu:~# apt-get install ewf-tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libbfio1 libewf2
The following NEW packages will be installed:
  ewf-tools libbfio1 libewf2
0 upgraded, 3 newly installed, 0 to remove and 146 not upgraded.
Need to get 1,396 kB of archives.
After this operation, 8,554 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

61. ábra

Az alkalmazás telepítése az apt-get install ewf-tools paranccsal

Forrás: A szerző szerkesztése

Ezután futtassuk az ewfacquire parancsot. Ennek rengeteg kapcsolója van, de szerencsére nagy részük nem kötelező, hanem megkérdezi őket, ha nem adjuk meg.

Indítsuk el a másolást. A következő kapcsolók fontosabbak:

- Másolás forrása mindig az utolsó paraméter, kapcsoló nélkül, például: /dev/sdb
- Másolás célja -t, például: -t /mnt/image1

Javasolt még megadni a -d kapcsolóval azt, hogy milyen egyéb hashértéket számoljon. Ezt azért adjuk meg, mert nem kérdezi meg interaktívan, ha nem adjuk meg kapcsolóval.

A többi paraméter, amit megkérdez:

- *Case Number:* egy ügyszám, általában meg van adva, azt használjuk.
- *Description:* leírás az ügyről, a számítógépről. Próbáljunk meg minden hasznos információt leírni, ami úgy érezzük, hogy a későbbi vizsgálatot segítheti. Körülmények, leírás a gépről, nevek, milyen jellegű információt kell keresni, ha tudjuk.
- *Evidence Number:* a bizonyíték száma. Általában adott helyszínen belül 1-től kezdve sorszámozunk.
- *Examiner name:* a lefoglalást végző szakértő neve, szakértői igazolvány száma esetleg.
- *Notes:* bármi egyéb megjegyzés, amit fontosnak tartunk.
- *Media type:* miről készült a másolat merevlemez, dvd, USB.
- *Media characteristics:* egész adathordozót másoltunk physical, vagy partíciót logical.
- *File format:* készítendő másolat formátuma. Különböző formátumok más más hashfajtákat támogatnak, más tömörítési lehetőségek vannak.
- *Compression method:* a tömörítés módja. Általában nem javasolt tömöríteni, hacsak nincs kevés helyünk.
- *Compression level:* a tömörítés mértéke.

- *Start offset:* milyen offsettől kezdjen el másolni? Általában az egész eszközt másoljuk, tehát 0 legyen.
- *Number of bytes to acquire:* hány byteot másoljon? Általában az egész eszközt másoljuk, válasszuk a felajánlott értéket, mert az az alapértelmezés.
- *Evidence segment filesize:* mekkora darabokra tördelje az eredményt?
- *Bytes per sector:* egy szektort hány byte alkot? Szinte mindig 512. Rá van írva a merevlemezre, illetve az fdisk -l parancs kiírja.
- *Sectors to read at once:* egyszerre hány szektort olvasson?
- *Error granuality:* milyen gyakorisággal tegyen le ellenőrző hashértéket?
- *Retries when read error occures:* ha hiba történik egy szektor olvasásakor, hányszor próbálja újra?
- *Wipe sectors on read error:* Ha nem lehet egy szektort olvasni, azt null byteokkal feltöltöttnek mentse-e?

```
root@ubuntu: ~
root@ubuntu:~# ewfacquire -t /mnt/image1 -d sha256 /dev/sdb
ewfacquire 20140608

Device information:
Bus type:                                       ATA/ATAPI
Vendor:                                         ATA
Model:                                          VBOX HARDDISK
Serial:                                         VB3915741a-058dcbfc

Storage media information:
Type:                                           Device
Media type:                                     Fixed
Media size:                                     1.0 GB (1073741824 bytes)
Bytes per sector:                               512

Acquiry parameters required, please provide the necessary input
Case number: 2017.01.01-01-asdfg
Description: asztaligep
Evidence number: 1
Examiner name: x y
Notes: egyeb
Media type (fixed, removable, optical, memory) [fixed]:
Media characteristics (logical, physical) [physical]:
Use EWF file format (ewf, smart, ftk, encase1, encase2, encase3, encase4, encase5,
 encase6, linen5, linen6, ewfx) [encase6]: ewfx
Compression method (deflate) [deflate]:
```

```
Compression method (deflate) [deflate]:
Compression level (none, empty-block, fast, best) [none]:
Start to acquire at offset (0 <= value <= 1073741824) [0]:
The number of bytes to acquire (0 <= value <= 1073741824) [1073741824]:
Evidence segment file size in bytes (1.0 MiB <= value <= 1.9 GiB) [1.4 GiB]: 512M
The number of bytes per sector (1 <= value <= 4294967295) [512]:
The number of sectors to read at once (16, 32, 64, 128, 256, 512, 1024, 2048, 4096
, 8192, 16384, 32768) [64]:
The number of sectors to be used as error granularity (1 <= value <= 64) [64]:
The number of retries when a read error occurs (0 <= value <= 255) [2]:
Wipe sectors on read error (mimic EnCase like behavior) (yes, no) [no]: yes

The following acquiry parameters were provided:
Image path and filename:                /mnt/image1.e01
Case number:                            2017.01.01-01-asdfg
Description:                            asztaligep
Evidence number:                        1
Examiner name:                          x y
Notes:                                  egyeb
Media type:                             fixed disk
Is physical:                            yes
EWF file format:                        extended EWF (ewfx) (.e01)
Compression method:                     deflate
Compression level:                      none
Acquiry start offset:                   0
Number of bytes to acquire:             1.0 GiB (1073741824 bytes)
```

```
Acquiry start offset:                    0
Number of bytes to acquire:              1.0 GiB (1073741824 bytes)
Evidence segment file size:              512 MiB (536870912 bytes)
Bytes per sector:                        512
Block size:                              64 sectors
Error granularity:                       64 sectors
Retries on read error:                   2
Zero sectors on read error:              yes

Continue acquiry with these values (yes, no) [yes]:

Acquiry started at: Mar 15, 2017 20:51:25
This could take a while.

Status: at 27%.
        acquired 283 MiB (297304064 bytes) of total 1.0 GiB (1073741824 bytes).
        completion in 10 second(s) with 73 MiB/s (76695844 bytes/second).

Status: at 60%.
        acquired 618 MiB (648118272 bytes) of total 1.0 GiB (1073741824 bytes).
        completion in 5 second(s) with 78 MiB/s (82595524 bytes/second).

Status: at 91%.
        acquired 941 MiB (987004928 bytes) of total 1.0 GiB (1073741824 bytes).
        completion in 1 second(s) with 78 MiB/s (82595524 bytes/second).
```

```
Acquiry completed at: Mar 15, 2017 20:51:38

Written: 1.0 GiB (1073742255 bytes) in 13 second(s) with 78 MiB/s (82595558 bytes/
second).
MD5 hash calculated over data:          a1e6b4971646cd6acc40a05470525dcb
SHA256 hash calculated over data:       9758e017d07569106ce29013464e79615859c741aa
e6eaa2d7849413de5897f1
ewfacquire: SUCCESS
root@ubuntu:~#
```

62. ábra

Az ewfacquire parancs futtatása

Forrás: A szerző szerkesztése

Ahogy eddig, a hashértéket mindenképpen foglaljuk bele a házkutatási jegyzőkönyvbe is. Erre azért van szükség, mert a hash csak a véletlen módosulás ellen véd, a szándékosság ellen nem. Tehát egy rosszindulatú elemző visszaállíthatja a raw imaget, bizonyítékot helyez el benne vagy távolít el, majd erről az új változatról készít imaget, és az eredetit erre kicseréli. Az ilyen beavatkozások ellen véd a több tanú által aláírt, helyszínen készült jegyzőkönyv.

Ellenőrizzük, milyen fájlokat kaptunk!

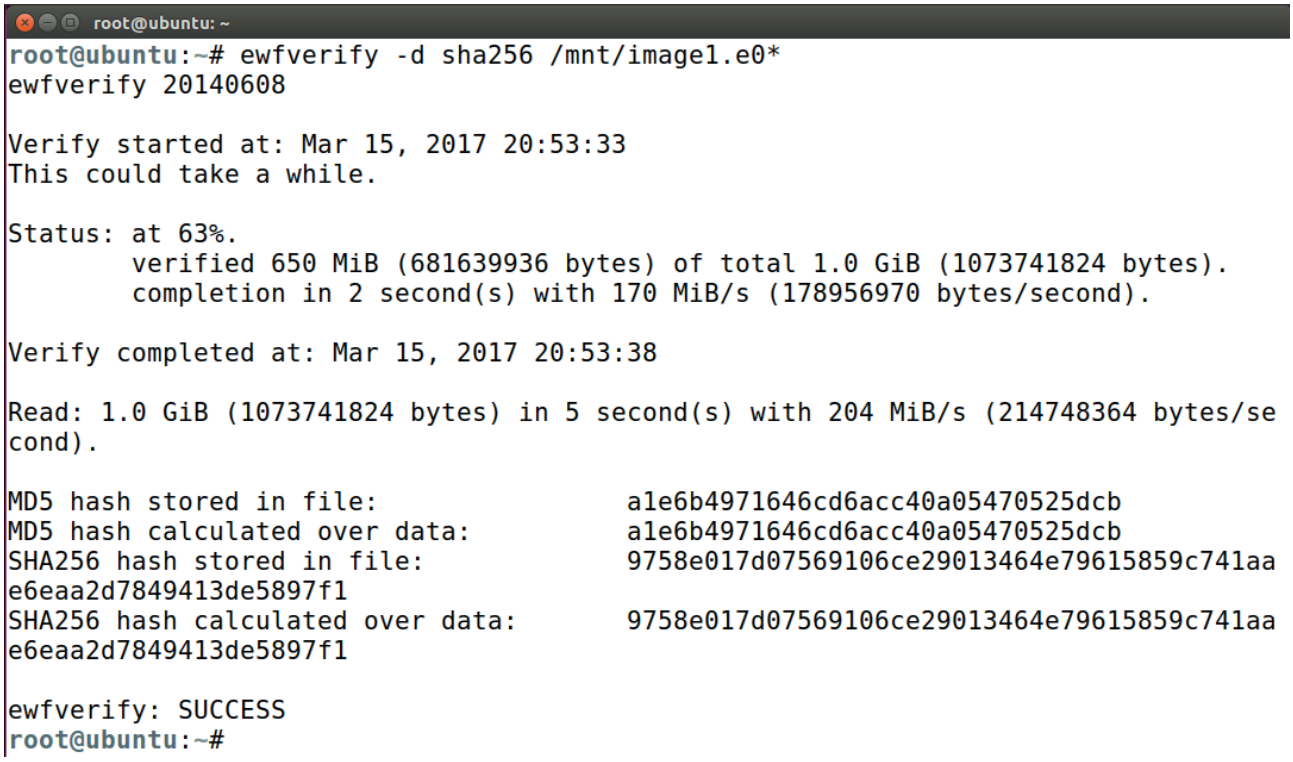
```
root@ubuntu: ~
root@ubuntu:~# ls -la /mnt/
total 1048980
drwxrwxrwx  1 root root      4096 Mar 15 20:51 .
drwxr-xr-x 24 root root      4096 Jan 14 12:52 ..
-rwxrwxrwx  1 root root 536840140 Mar 15 20:51 image1.e01
-rwxrwxrwx  1 root root 536839561 Mar 15 20:51 image1.e02
-rwxrwxrwx  1 root root    460776 Mar 15 20:51 image1.e03
root@ubuntu:~#
```

63. ábra

A kapott fájlok ellenőrzése

Forrás: A szerző szerkesztése

Amennyiben később ellenőrizni szeretnénk, hogy sérült-e az image, futtassuk az ewfverify parancsot.



64. ábra

Az ewfverify parancs futtatása

Forrás: A szerző szerkesztése

Ha valami sérülés történik, az ewfverify megadja, hogy melyik szektorok hibásak.

```
root@ubuntu: ~
root@ubuntu:~# ewfverify -d sha256 /mnt/image1.e0*
ewfverify 20140608

Verify started at: Mar 17, 2017 16:39:56
This could take a while.

Status: at 52%.
        verified 532 MiB (558596096 bytes) of total 1.0 GiB (1073741824 bytes).
        completion in 3 second(s) with 146 MiB/s (153391689 bytes/second).

Verify completed at: Mar 17, 2017 16:40:02

Read: 1.0 GiB (1073741824 bytes) in 6 second(s) with 170 MiB/s (178956970 bytes/
second).

Sector validation errors:
        total number: 1
        at sector(s): 128 - 191 (number: 64) in segment file(s): /mnt/image1.e01

MD5 hash stored in file:                a1e6b4971646cd6acc40a05470525dcb
MD5 hash calculated over data:          2b711ae47d51225668ceef0571d3057f
SHA256 hash stored in file:             9758e017d07569106ce29013464e79615859c741
aae6eaa2d7849413de5897f1
SHA256 hash calculated over data:       06753a54d4011afc34206488256d1bc9a5c221fa
aa50ff2fc032923b3534065f

Unable to verify input.
ewfverify: FAILURE
root@ubuntu:~#
```

65. ábra

A hibás szektorok kimutatása

Forrás: A szerző szerkesztése

9.3. Memória Image vizsgálata

A memória image, amennyiben tudtunk készíteni, rengeteg hasznos adatot tartalmazhat. A legfontosabbak, amikhez lényegében máshogyan nem juthatunk hozzá azok, a titkosító kulcsok a full disk titkosításokhoz (mint bitlocker, truecrypt veracrypt); valamint a nyílt szövegben tárolt jelszavak. De ezeken kívül nagyon fontos malwareanalízis során is, rejtett processek és kapcsolatok megtalálása miatt, melyek éppen mondjuk egy ártatlanságot bizonyíthatnak, például kiderül, hogy egy Zeus vírus végezte az átutalást.

9.3.1. Volatility

A legelterjedtebb memóriadump-analizáló eszköz a volatility. Rengeteg alkalmazás használja a háttérben, és sok kiegészítő található hozzá az interneten.

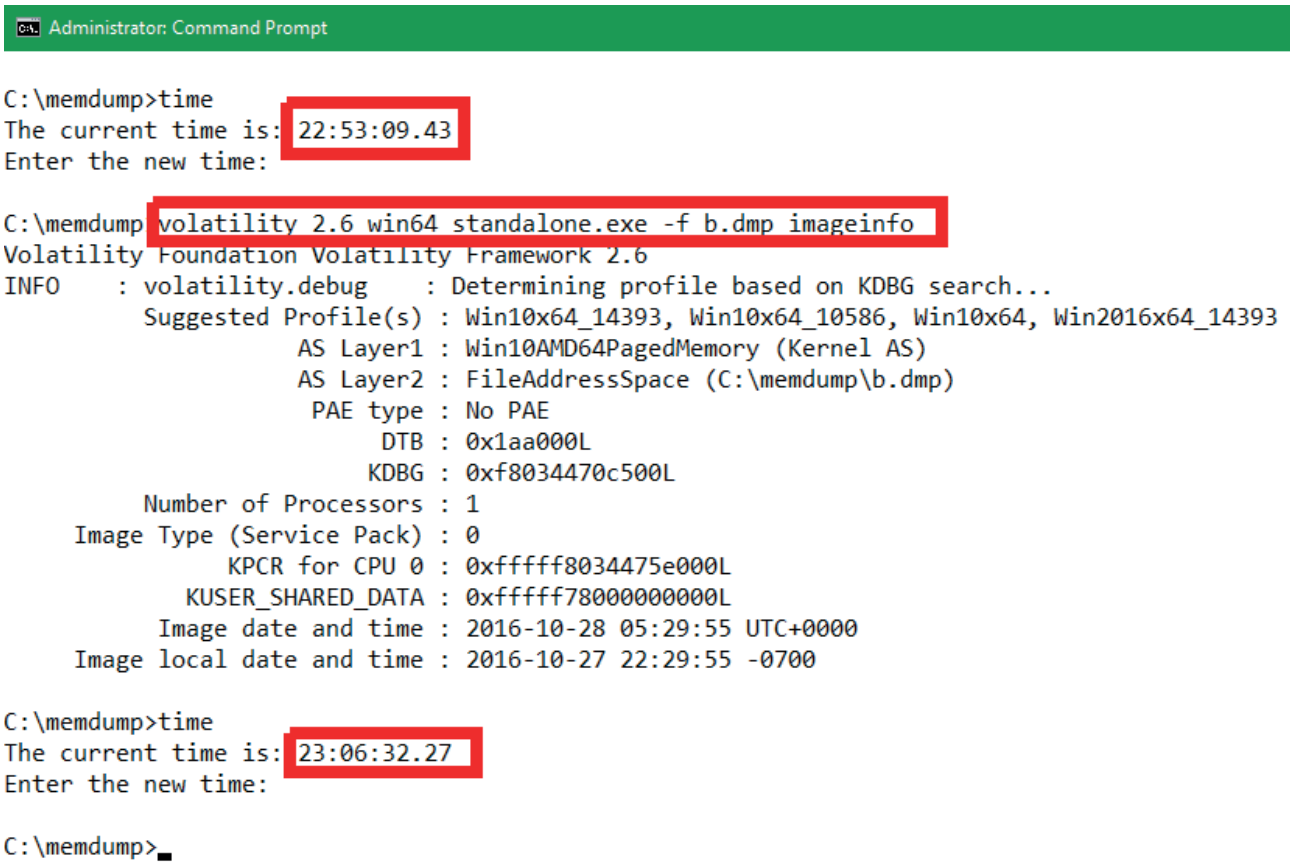
Most nézzük meg, milyen analíziseket végezhetünk a segítségével, és abból miket tudhatunk meg!

9.4.1.1. Operációs rendszer verziójának megállapítása volatilityvel

Az első és legfontosabb lépés minden memóriaanalízis kezdete előtt, hogy megállapítsuk, milyen operációs rendszerről készült. Ez remélhetőleg benne van a megkapott információk között is, de mindenképpen ellenőrizzük mi is, és vessük össze a kapott információval. Járjunk utána, ha eltérés van, annak mi lehet az oka!

Ez a lépés azért szükséges, hogy későbbi parancsoknál megadhassuk a használandó profilt a --profile kapcsoló segítségével, ami jelentősen felgyorsítja a futást, illetve néhány parancs hibásan fut(hat), ha nem adjuk meg.

Ezt a korábban már említett volatility -f <memory image file neve> imageinfo paranccsal tehetjük meg. A parancs elég hosszú ideig fut.



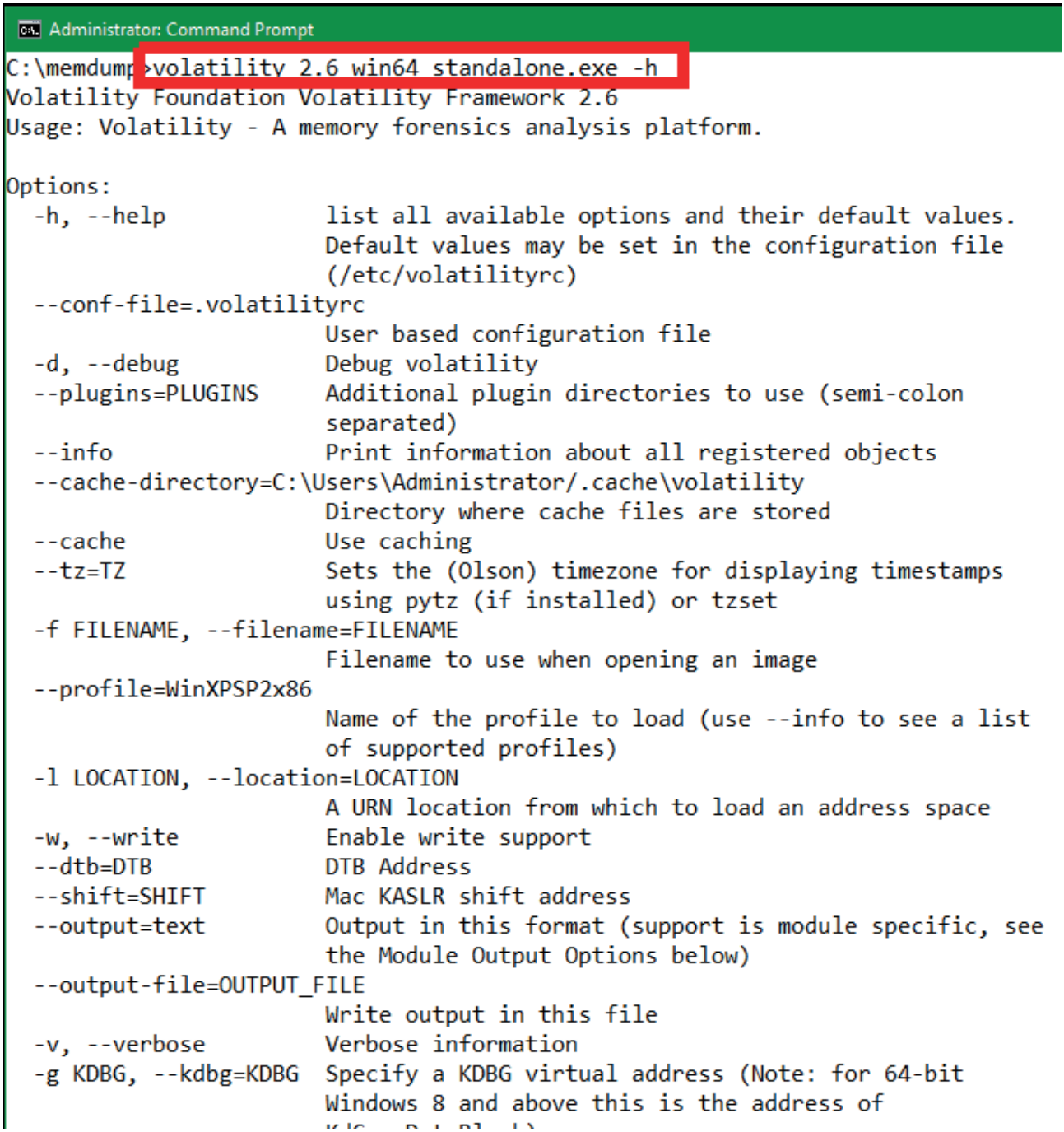
66. ábra

A volatility -f <memory image file neve> imageinfo parancs futtatása

Forrás: A szerző szerkesztése

9.4.1.2. A volatility helpje

Felmerülhet, abszolút jogosan, hogy miért említem meg külön a help használatát, hiszen azt nagy valószínűséggel azért mindenki megtalálja magától is. Az ok egy lehetséges buktató. *Volatility esetében a különböző profilokhoz más-más help tartozik.* Ha belegondolunk, ez valahol logikus, hiszen más-más operációs rendszereknél, kernelverzióknál más-más adatstruktúrák léteznek, tehát mást és máshogyan lehet kinyerni. Ezért nagyon fontos, hogy amikor csak simán kiadjuk a volatility -h parancsot, a default (az általam használt verziónál windows XP SP2) profilhoz tartozó helpet kapjuk meg.


Administrator: Command Prompt
C:\memdump>volatility_2.6_win64_standalone.exe -h
Volatility Foundation Volatility Framework 2.6
Usage: Volatility - A memory forensics analysis platform.
Options:
-h, --help list all available options and their default values.
Default values may be set in the configuration file
(/etc/volatilityrc)
--conf-file=.volatilityrc
User based configuration file
-d, --debug Debug volatility
--plugins=PLUGINS Additional plugin directories to use (semi-colon
separated)
--info Print information about all registered objects
--cache-directory=C:\Users\Administrator/.cache\volatility
Directory where cache files are stored
--cache Use caching
--tz=TZ Sets the (Olson) timezone for displaying timestamps
using pytz (if installed) or tzset
-f FILENAME, --filename=FILENAME
Filename to use when opening an image
--profile=WinXPSP2x86
Name of the profile to load (use --info to see a list
of supported profiles)
-l LOCATION, --location=LOCATION
A URN location from which to load an address space
-w, --write Enable write support
--dtb=DTB DTB Address
--shift=SHIFT Mac KASLR shift address
--output=text Output in this format (support is module specific, see
the Module Output Options below)
--output-file=OUTPUT_FILE
Write output in this file
-v, --verbose Verbose information
-g KDBG, --kdbg=KDBG Specify a KDBG virtual address (Note: for 64-bit
Windows 8 and above this is the address of

```
-g KDBG, --kdbg=KDBG  Specify a KDBG virtual address (Note: for 64-bit
                      Windows 8 and above this is the address of
                      KdCopyDataBlock)
--force               Force utilization of suspect profile
-k KPCR, --kpcr=KPCR  Specify a specific KPCR address
--cookie=COOKIE       Specify the address of nt!ObHeaderCookie (valid for
                      Windows 10 only)

      Supported Plugin Commands:

              amcache         Print AmCache information
              apihooks        Detect API hooks in process and kernel memory
              atoms           Print session and window station atom tables
              atomscan        Pool scanner for atom tables
              auditpol        Prints out the Audit Policies from HKLM\SECURITY\Policy\PolAdtEv
              bigpools        Dump the big page pools using BigPagePoolScanner
              bioskbd         Reads the keyboard buffer from Real Mode memory
              cachedump       Dumps cached domain hashes from memory
              callbacks       Print system-wide notification routines
              clipboard       Extract the contents of the windows clipboard
              cmdline         Display process command-line arguments
              cmdscan         Extract command history by scanning for _COMMAND_HISTORY
              connections     Print list of open connections [Windows XP and 2003 Only]
              connscan        Pool scanner for tcp connections
              consoles        Extract command history by scanning for _CONSOLE_INFORMATION
              crashinfo       Dump crash-dump information
              deskscan        Poolscaner for tagDESKTOP (desktops)
              devicetree      Show device tree
              dlldump         Dump DLLs from a process address space
              dlllist         Print list of loaded dlls for each process
              driverirp       Driver IRP hook detection
              drivermodule    Associate driver objects to kernel modules
              driverscan      Pool scanner for driver objects
              dumpcerts       Dump RSA private and public SSL keys
              dumpfiles       Extract memory mapped and cached files
```

```
dumpregistry    Dumps registry files out to disk
editbox         Displays information about Edit controls. (Listbox experimental.)
envars          Display process environment variables
eventhooks      Print details on windows event hooks
evtlogs         Extract Windows Event Logs (XP/2003 only)
filescan        Pool scanner for file objects
gahti           Dump the USER handle type information
gditimers       Print installed GDI timers and callbacks
gdt             Display Global Descriptor Table
getservicesids  Get the names of services in the Registry and return Calculated SID
getsids         Print the SIDs owning each process
handles         Print list of open handles for each process
hashdump        Dumps passwords hashes (LM/NTLM) from memory
hibinfo         Dump hibernation file information
hivedump        Prints out a hive
hivelist        Print list of registry hives.
hivescan        Pool scanner for registry hives
hpakextract     Extract physical memory from an HPAK file
hpakinfo        Info on an HPAK file
idt             Display Interrupt Descriptor Table
iehistory       Reconstruct Internet Explorer cache / history
imagecopy       Copies a physical address space out as a raw DD image
imageinfo       Identify information for the image
impscan         Scan for calls to imported functions
joblinks        Print process job link information
kdbgscan        Search for and dump potential KDBG values
kpcrscan        Search for and dump potential KPCR values
ldrmodules      Detect unlinked DLLs
lsadump         Dump (decrypted) LSA secrets from the registry
machoinfo       Dump Mach-O file format information
malfind         Find hidden and injected code
mbrparser       Scans for and parses potential Master Boot Records (MBRs)
memdump         Dump the addressable memory for a process
memmap          Print the memory map
messagehooks    List desktop and thread window message hooks
```

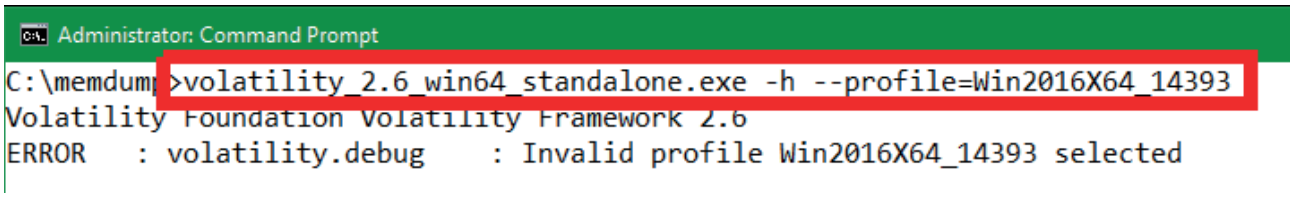
```
mftparser       Scans for and parses potential MFT entries
moddump         Dump a kernel driver to an executable file sample
modscan         Pool scanner for kernel modules
modules         Print list of loaded modules
multiscan       Scan for various objects at once
mutantscan      Pool scanner for mutex objects
notepad         List currently displayed notepad text
objtypescan     Scan for Windows object type objects
patcher         Patches memory based on page scans
poolpeek        Configurable pool scanner plugin
printkey        Print a registry key, and its subkeys and values
privs           Display process privileges
procdump        Dump a process to an executable file sample
pslist          Print all running processes by following the EPROCESS lists
psscan          Pool scanner for process objects
pstree          Print process list as a tree
psxview         Find hidden processes with various process listings
qemuinfo        Dump Qemu information
raw2dmp         Converts a physical memory sample to a windbg crash dump
screenshot      Save a pseudo-screenshot based on GDI windows
servicediff     List Windows services (ala Plugx)
sessions        List details on _MM_SESSION_SPACE (user logon sessions)
shellbags       Prints ShellBags info
shimcache       Parses the Application Compatibility Shim Cache registry key
shutdowntime    Print ShutdownTime of machine from registry
sockets         Print list of open sockets
sockscan        Pool scanner for tcp socket objects
ssdt            Display SSDT entries
strings         Match physical offsets to virtual addresses (may take a while, VERY verbose)
svcscan         Scan for Windows services
symlinkscan     Pool scanner for symlink objects
thrdscan        Pool scanner for thread objects
threads         Investigate _ETHREAD and _KTHREADs
timeliner       Creates a timeline from various artifacts in memory
timers          Print kernel timers and associated module DPCs

truecryptmaster Recover TrueCrypt 7.1a Master Keys
truecryptpassphrase     TrueCrypt Cached Passphrase Finder
truecryptsummary        TrueCrypt Summary
unloadedmodules Print list of unloaded modules
userassist      Print userassist registry keys and information
userhandles     Dump the USER handle tables
vaddump         Dumps out the vad sections to a file
vadinfo         Dump the VAD info
vadtree         Walk the VAD tree and display in tree format
vadwalk         Walk the VAD tree
vboxinfo        Dump virtualbox information
verinfo         Prints out the version information from PE images
vmwareinfo      Dump VMware VMSS/VMSN information
volshell        Shell in the memory image
windows         Print Desktop Windows (verbose details)
wintree         Print Z-Order Desktop Windows Tree
wndscan         Pool scanner for window stations
yarascan        Scan process or kernel memory with Yara signatures

C:\memdump>
```

67. ábra

A volatility -h parancs futtatása

Forrás: A szerző szerkesztése

Ezért, ha megvan az operációs rendszer típusa, futtasuk ismét a help lekérését a volatility -h --profile=<profile neve kis-NAGY betű helyesen>. Amennyiben hibásan írjuk a profilt, akkor a következő üzenetet kapjuk:



68. ábra

Hibásan írt profil esetén kapott üzenet

Forrás: A szerző szerkesztése

Ha helyesen írjuk, akkor pedig az adott profilhoz tartozó helpet látjuk.

```
Administrator: Command Prompt
C:\memdump>volatility_2.6_win64_standalone.exe -h --profile=Win2016x64_14393
Volatility Foundation Volatility Framework 2.6
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
                        (/etc/volatilityrc)
  --conf-file=.volatilityrc
                        User based configuration file
  -d, --debug           Debug volatility
  --plugins=PLUGINS     Additional plugin directories to use (semi-colon
                        separated)
  --info                Print information about all registered objects
  --cache-directory=C:\Users\Administrator/.cache\volatility
                        Directory where cache files are stored
  --cache               Use caching
  --tz=TZ               Sets the (Olson) timezone for displaying timestamps
                        using pytz (if installed) or tzset
  -f FILENAME, --filename=FILENAME
                        Filename to use when opening an image
  --profile=Win2016x64_14393
                        Name of the profile to load (use --info to see a list
                        of supported profiles)
  -l LOCATION, --location=LOCATION
                        A URN location from which to load an address space
  -w, --write           Enable write support
  --dtb=DTB             DTB Address
  --shift=SHIFT         Mac KASLR shift address
  --output=text         Output in this format (support is module specific, see
                        the Module Output Options below)
  --output-file=OUTPUT_FILE
                        Write output in this file
  -v, --verbose         Verbose information
```

```
-g KDBG, --kdbg=KDBG  Specify a KDBG virtual address (Note: for 64-bit
                      Windows 8 and above this is the address of
                      KdCopyDataBlock)
--force               Force utilization of suspect profile
--cookie=COOKIE       Specify the address of nt!ObHeaderCookie (valid for
                      Windows 10 only)
-k KPCR, --kpcr=KPCR  Specify a specific KPCR address

      Supported Plugin Commands:

              amcache         Print AmCache information
              apihooks        Detect API hooks in process and kernel memory
              atoms           Print session and window station atom tables
              atomscan        Pool scanner for atom tables
              auditpol        Prints out the Audit Policies from HKLM\SECURITY\Policy\PolAdtEv
              bigpools        Dump the big page pools using BigPagePoolScanner
              bioskbd         Reads the keyboard buffer from Real Mode memory
              cachedump       Dumps cached domain hashes from memory
              callbacks       Print system-wide notification routines
              clipboard       Extract the contents of the windows clipboard
              cmdline         Display process command-line arguments
              cmdscan         Extract command history by scanning for _COMMAND_HISTORY
              consoles        Extract command history by scanning for _CONSOLE_INFORMATION
              crashinfo       Dump crash-dump information
              deskscan        Poolscaner for tagDESKTOP (desktops)
              devicetree      Show device tree
              dlldump         Dump DLLs from a process address space
              dlllist         Print list of loaded dlls for each process
              driverirp       Driver IRP hook detection
              drivermodule    Associate driver objects to kernel modules
              driverscan      Pool scanner for driver objects
              dumpcerts       Dump RSA private and public SSL keys
              dumpfiles       Extract memory mapped and cached files
              dumpregistry    Dumps registry files out to disk
              editbox         Displays information about Edit controls. (Listbox experimental.)
              envars          Display process environment variables
```

```
eventhooks      Print details on windows event hooks
filescan        Pool scanner for file objects
gahti           Dump the USER handle type information
getservicesids  Get the names of services in the Registry and return Calculated SID
getsids         Print the SIDs owning each process
handles         Print list of open handles for each process
hashdump        Dumps passwords hashes (LM/NTLM) from memory
hibinfo         Dump hibernation file information
hivedump        Prints out a hive
hivelist        Print list of registry hives.
hivescan        Pool scanner for registry hives
hpakextract     Extract physical memory from an HPAK file
hpakinfo        Info on an HPAK file
iehistory       Reconstruct Internet Explorer cache / history
imagecopy       Copies a physical address space out as a raw DD image
imageinfo       Identify information for the image
impscan         Scan for calls to imported functions
joblinks        Print process job link information
kdbgscan        Search for and dump potential KDBG values
kpcrscan        Search for and dump potential KPCR values
ldrmodules      Detect unlinked DLLs
lsadump         Dump (decrypted) LSA secrets from the registry
machoinfo       Dump Mach-O file format information
malfind         Find hidden and injected code
mbrparser       Scans for and parses potential Master Boot Records (MBRs)
memdump         Dump the addressable memory for a process
memmap          Print the memory map
messagehooks    List desktop and thread window message hooks
mftparser       Scans for and parses potential MFT entries
moddump         Dump a kernel driver to an executable file sample
modscan         Pool scanner for kernel modules
modules         Print list of loaded modules
multiscan       Scan for various objects at once
mutantscan      Pool scanner for mutex objects
netscan         Scan a Vista (or later) image for connections and sockets
```

```
objtypescan     Scan for Windows object type objects
patcher         Patches memory based on page scans
poolpeek        Configurable pool scanner plugin
pooltracker     Show a summary of pool tag usage
printkey        Print a registry key, and its subkeys and values
privs           Display process privileges
procdump        Dump a process to an executable file sample
pslist          Print all running processes by following the EPROCESS lists
psscan          Pool scanner for process objects
pstree          Print process list as a tree
psxview         Find hidden processes with various process listings
qemuinfo        Dump Qemu information
raw2dmp         Converts a physical memory sample to a windbg crash dump
screenshot      Save a pseudo-screenshot based on GDI windows
sessions        List details on _MM_SESSION_SPACE (user logon sessions)
shellbags       Prints ShellBags info
shimcache       Parses the Application Compatibility Shim Cache registry key
shutdowntime    Print ShutdownTime of machine from registry
ssdt            Display SSDT entries
strings         Match physical offsets to virtual addresses (may take a while, VERY verbose)
svcscan         Scan for Windows services
symlinkscan     Pool scanner for symlink objects
thrdscan        Pool scanner for thread objects
threads         Investigate _ETHREAD and _KTHREADs
timeliner       Creates a timeline from various artifacts in memory
timers          Print kernel timers and associated module DPCs
truecryptmaster Recover TrueCrypt 7.1a Master Keys
truecryptpassphrase     TrueCrypt Cached Passphrase Finder
truecryptsummary        TrueCrypt Summary
unloadedmodules Print list of unloaded modules
userassist      Print userassist registry keys and information
userhandles     Dump the USER handle tables
vaddump         Dumps out the vad sections to a file
vadinfo         Dump the VAD info
vadtree         Walk the VAD tree and display in tree format
vadwalk         Walk the VAD tree
vboxinfo        Dump virtualbox information
verinfo         Prints out the version information from PE images
vmwareinfo      Dump VMware VMSS/VMSN information
volshell        Shell in the memory image
win10cookie     Find the ObHeaderCookie value for Windows 10
windows         Print Desktop Windows (verbose details)
wintree         Print Z-Order Desktop Windows Tree
wndscan         Pool scanner for window stations
yarascan        Scan process or kernel memory with Yara signatures

C:\memdump>
```

69. ábra

Az adott profilhoz tartozó help

Forrás: A szerző szerkesztése

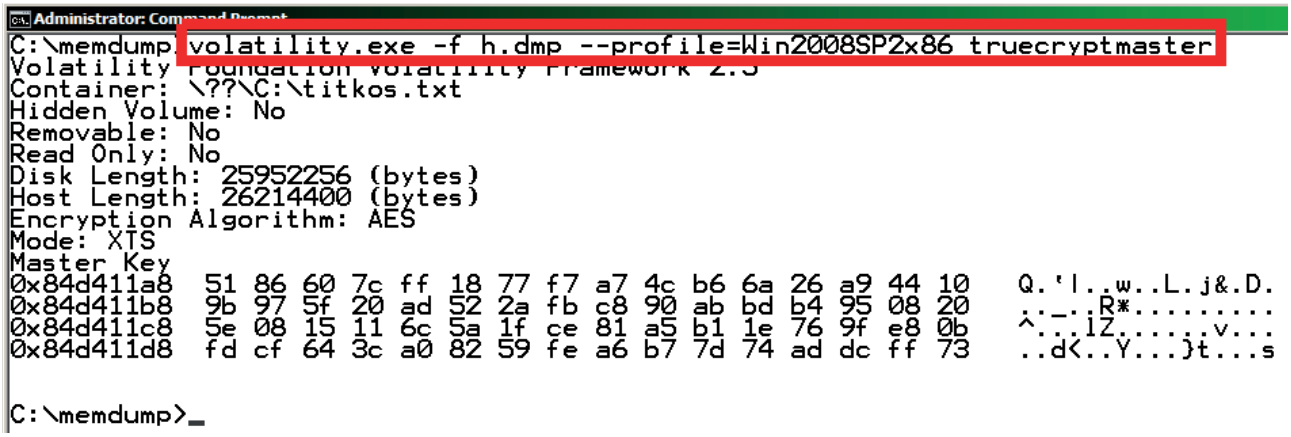
Vessük össze a két helpet. Például, az első helpben van conscan parancs, de nincs netscan parancs, míg a második helpben pont fordítva.

9.4.1.3. A Truecrypt (veracrypt) kulcs megszerzése memóriadumpból

Most már, hogy tisztában vagyunk az alapvető használattal, nézzünk néhány példát. Először is szerezzünk meg például egy truecrypt kulcsot. Fontos tudni, hogy ilyet csak akkor tudunk megszerezni, ha a memóriadump készítésekor a titkosított kötet fel volt csatolva.

A mesterkulcs megszerzéséhez használjuk a truecryptmaster parancsot:

volatility --profile=<profile neve kis-NAGY betű helyesen> -f <memoria dumpfile neve> truecryptmaster



70. ábra

A mesterkulcs megszerzése

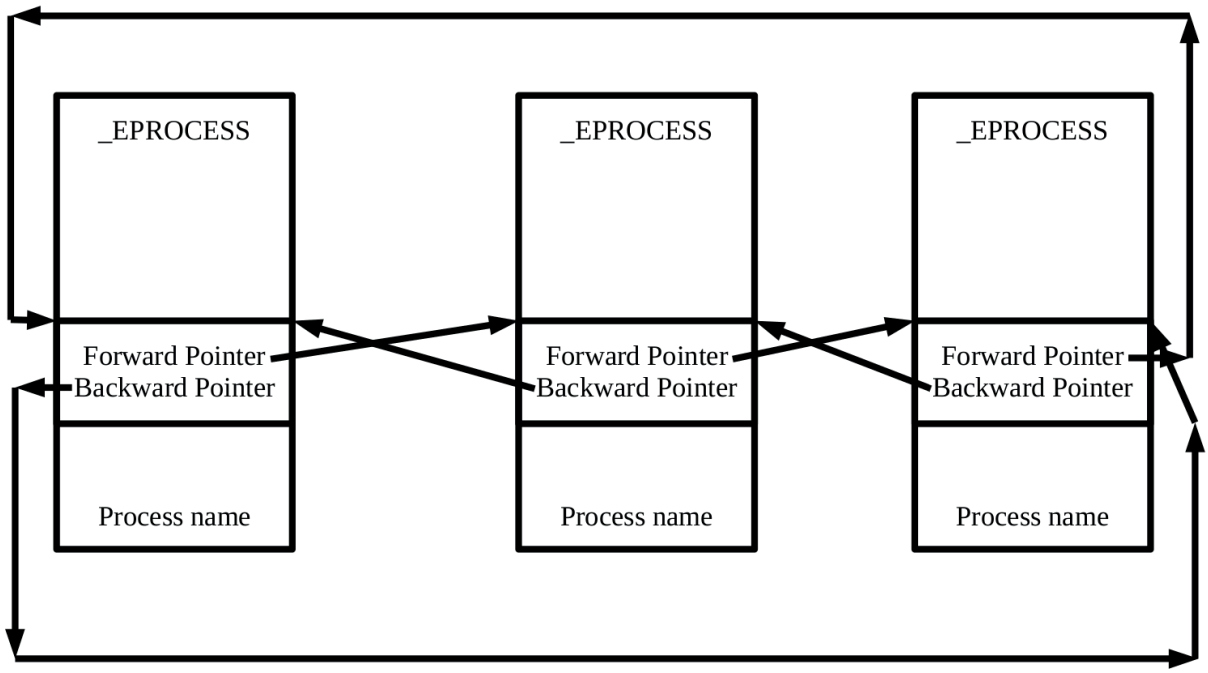
Forrás: A szerző szerkesztése

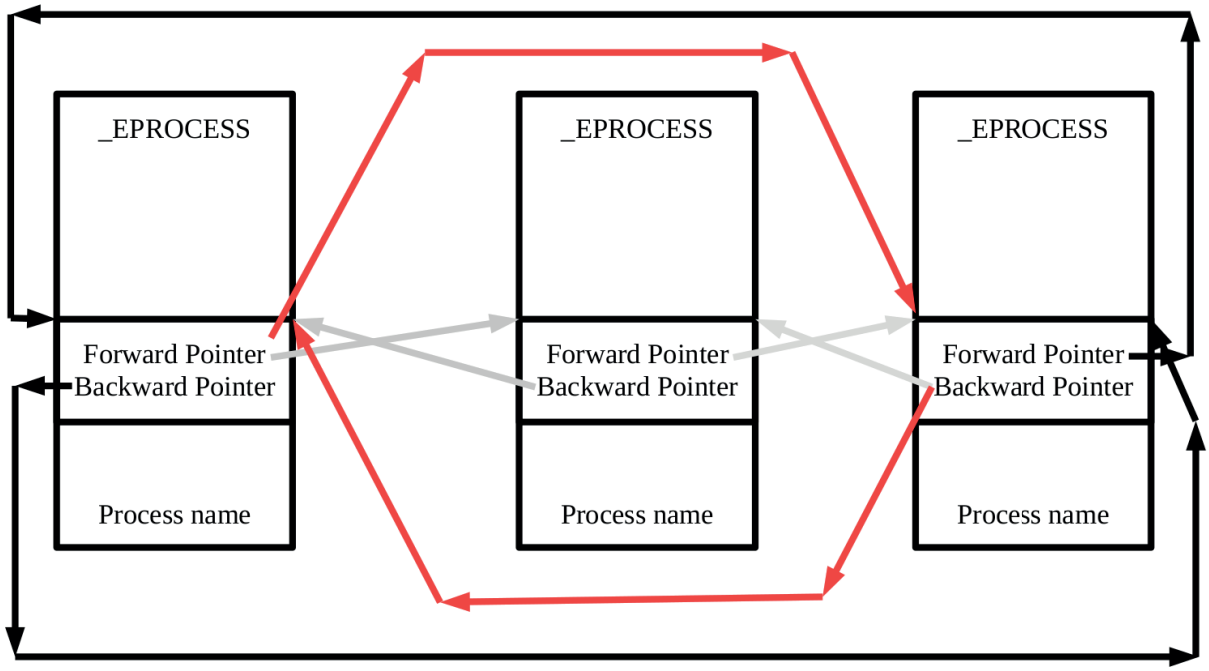
Ebből megkapjuk az AES kulcsot, amit a truecrypt használ, és segítségével visszafejthetjük az adatot. Az igazat megvallva, egyszerűbb egy alkalmazást használni rá, mint kézzel dolgoznunk, például a lostpassword kit, lásd később, teljesen automatizáltan és jobban (nem csak AES, hanem egyéb serpent, twofish kulcsokat is kezel, ismeri a veracryptet is, a volatility aktuális verziója nem) elvégzi ugyanezt a munkát.

9.4.1.4. Rejtett process megtalálása memóriadumpból

Processeket többféle módon is el tudunk rejteni. Az egyik elterjedt módszer a DKOM (Direct Kernel Object Modification). Ez úgy működik, hogy minden elindított processhez a kernel létrehoz egy úgynevezett _EPROCESS objektumot, ami leírja, milyen process, kinek a nevében, milyen jogokkal (token) indul. Ezek az _EPROCESS objektumok egy kétirányú láncolt listába vannak szervezve.

Egy processt úgy tudunk elrejteni, hogy kilinkeljük ebből a kétirányú láncolt listából:



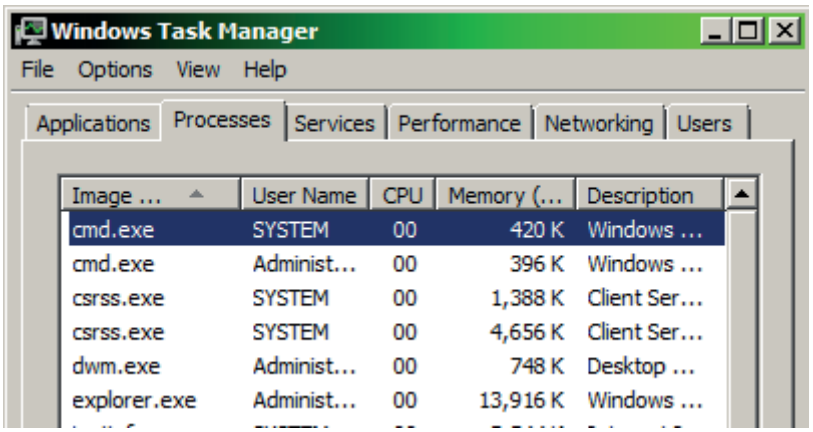


Ezt természetesen megvalósíthatjuk programból, de amennyiben csak tesztelni akarunk, ahhoz elegendő a Microsoft windbg nevű debuggere. Mivel nem tartozik szorosan a témához, ezért csak az utasításokat írom le, képernyőképek nélkül, felsorolás jelleggel:

– telepítsük fel a windbg-t;
– telepítsük fel az operációs rendszerünkhöz tartozó symbolfájlokat;
– állítsuk be, hogy a windbg használja a symbol fájlokat;

- állítsuk be az operációsrendszert, hogy támogassa a kerneldebuggingot (parancssorban bcdedit -debug on);
- indítsuk újra a gépet;
- indítsuk el a windbg-t;
- kezdjük el a kerneldebuggingot (fájl/kernel debug);
- keressük meg a láncolt lista elejét windbg-ben: dl nt!PsInitialSystemProcess a kiírt eredmények közül az első sorból a második pointer kell, ami pont a system process _EPROCESS objektumára mutat;
- írassuk ki az ott található adatokat, mint _EPROCESS objektumot (kizárólag a process névre, és a forward-backward pointerekre van szükségünk): dt _EPROCESS pointer -n ImageFileName -n ActiveProcessLinks;
- válasszunk egy irányt (forward vagy backward), és ahhoz a jövőben ragaszkodjunk. Én backward pointer írok, de értelemszerűen, aki a másik irányt választja, azt használja;
- ugorjunk a következő processre. Ne felejtsük el, hogy a pointer nem a következő _EPROCESS objektum elejére mutat, hanem ezen a struktúrán belül a következő ActualProcessLink objektum elejére, ezért annak a relatív offsetjét ki kell vonni. 2016 build 14393 esetében ez 0x2F0 volt: dt _EPROCESS backwardPointer-0x2f0 -n ImageFileName -n ActiveProcessLinks;
- ellenőrizzük, hogy arra a processre érkeztünk-e, amit el akarunk rejteni, ha nem, akkor ismét lépjünk a következő processre.

A calc.exe process el van rejtve a processlistából.

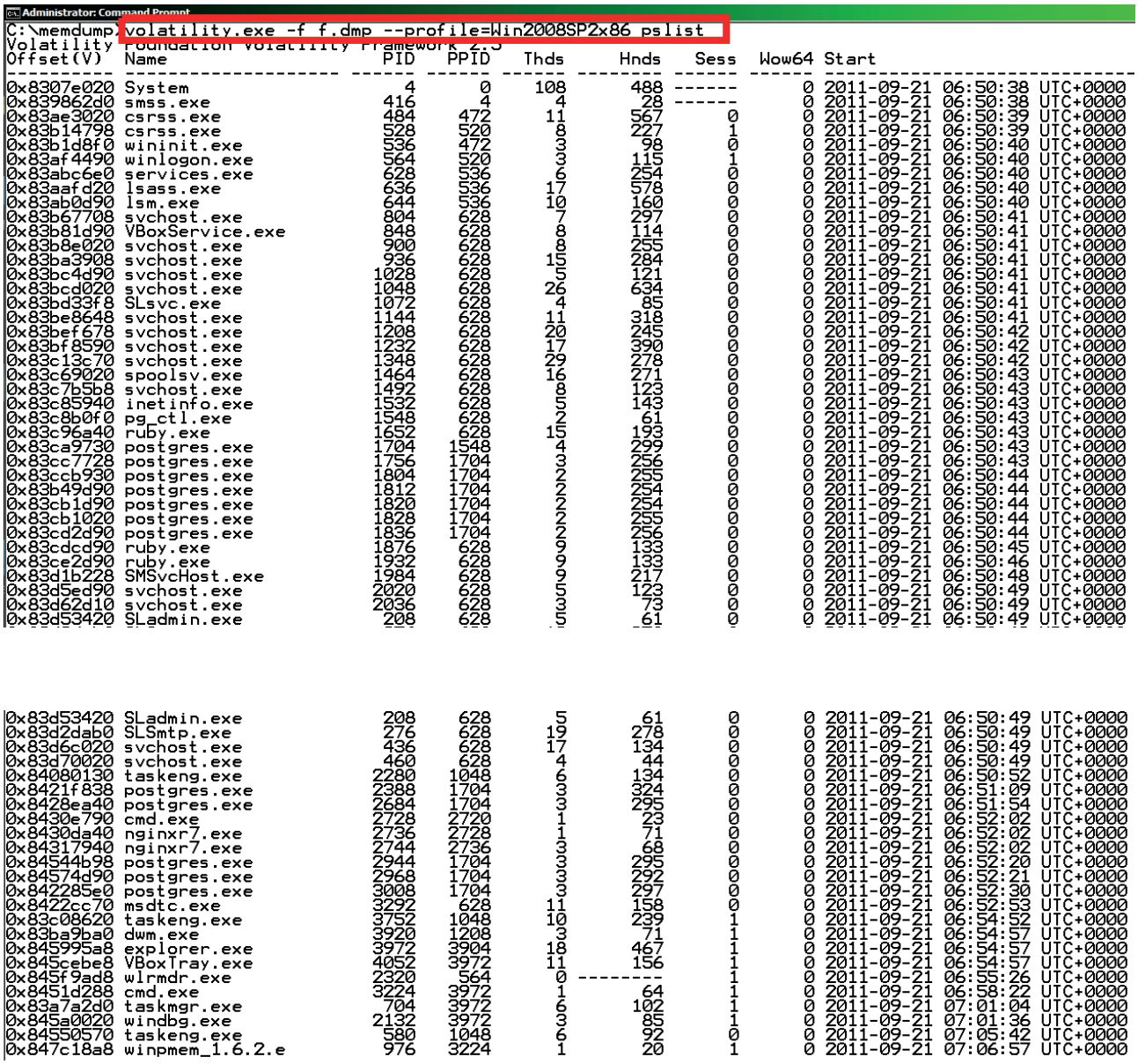


71. ábra

A calc.exe process hiánya

Forrás: A szerző szerkesztése

Memóriadumpból a volatilityvel a következő módon listázhatjuk a processeket: volatility -f <memória dump file neve> --profile=<profile neve kis-NAGY betű helyesen> pslist. Ekkor ugyanazt a listát kapjuk, mint amit windowsban is látunk taskmanager-rel, és szintén hiányzik belőle a win32calc.exe alkalmazás.

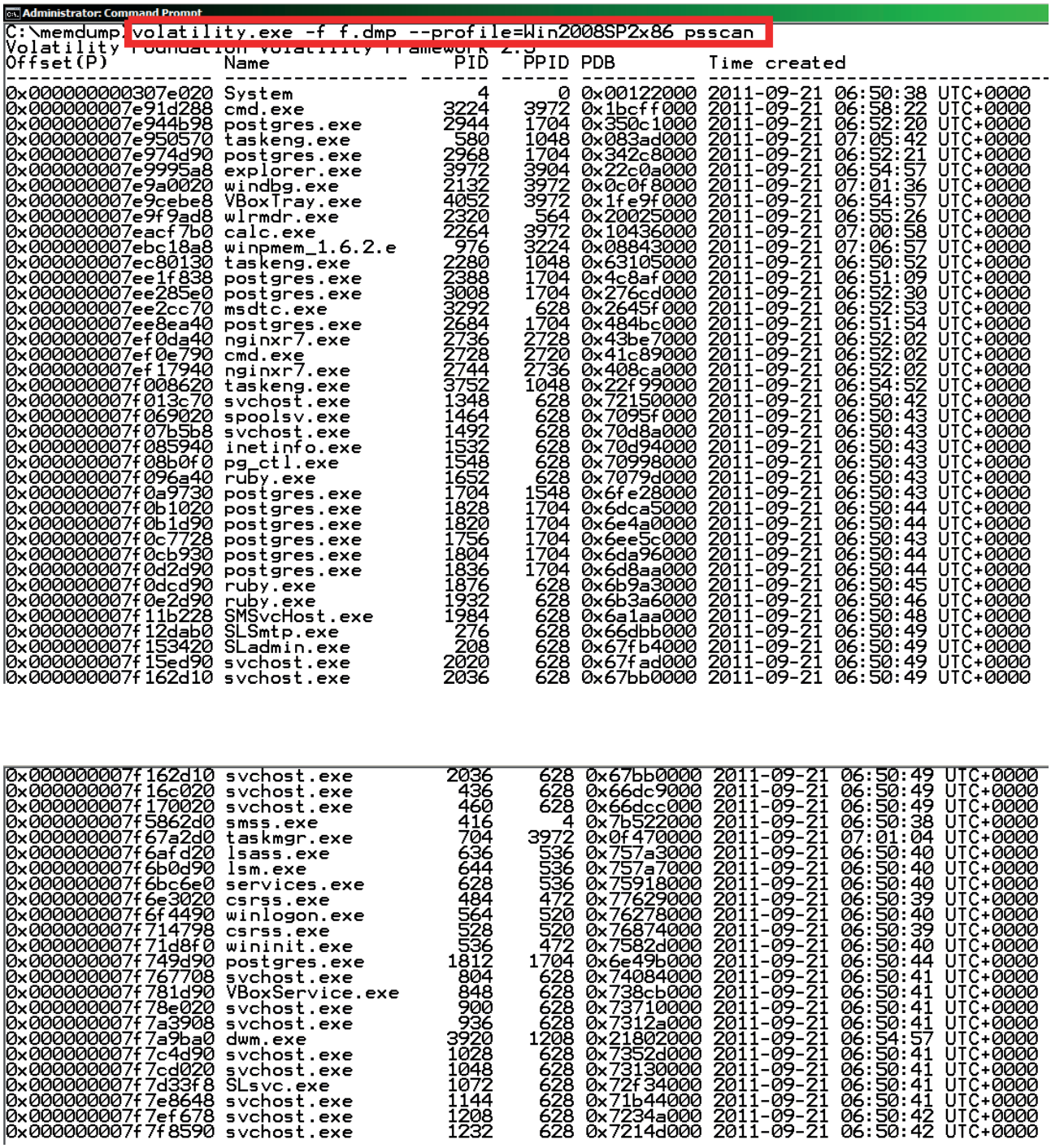


72. ábra

Proccesserek listázása volatilityvel

Forrás: A szerző szerkesztése

De van egy másik parancsunk is, a psscan, ami a memóriadumpot végigkeresi futó process struktúrák után (_EPROCESS objektum). Használjuk ezt is volatility -f <memória dump file neve> --profile=<profile neve kis-NAGY betű helyesen> psscan



73. ábra

A psscan parancs

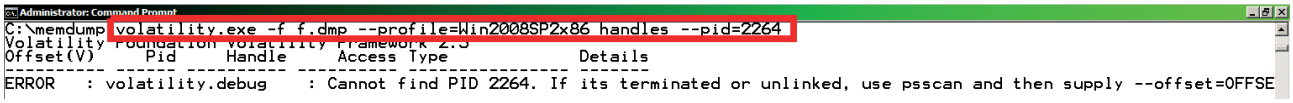
Forrás: A szerző szerkesztése

Vessük össze a két listát, és megtaláljuk a rejtett processt. A második lista mindig többet tartalmaz, mint az első, mert például az _EPROCESS objektum áthelyeződött.

Hogy ne kelljen manuálisan összehasonlítani a listákat, van egy psxview parancs: volatility -f <memória dump file neve> --profile=<profile neve kis-NAGY betű helyesen> psxview.

9.4.1.5. A processek által használt erőforrások megtalálása

Miután megtaláltuk a rejtett processt, a következő lépés, hogy megnézzük, vajon miket csinál. Windows alatt ezt úgy tehetjük meg, hogy megkeressük, a process milyen handleket használ. Ez azért hasznos, mert windows programozás során, ha valamilyen erőforráshoz (például fájl, registry kulcs, másik process, mutex) hozzá szeretnénk férni, az úgy történik, hogy kérünk az adott erőforráshoz egy handlet, és utána a különböző parancsoknál mindig ezt a handlet adjuk meg, így hivatkozunk az adott erőforrásra. Ha egy process handlejeit kiíratjuk, képet kapunk arról, mit csinált a memóriadump készítésének pillanatában (fontos, hogy ez egy pillanatkép, csak azt látjuk, milyen erőforrásokat használt a memóriadump-készítés pillanatában, nem korábban vagy később). A volatility lehetőséget ad nekünk ezen információk összegyűjtésére a handleskapcsolóval. Amennyiben magában használjuk, az összes process összes handlejét ki fogja írni, ami túl sok. Ezért általában a --pid= kapcsolóval együtt használjuk, ahol megadjuk, melyik process ID-jű folyamat handlejeire vagyunk kíváncsiak. Amennyiben a process rejtett, akkor a --pid= kapcsoló nem működik. Az én példám a következő: volatility.exe -f f.dmp --profile=Win2008SP2x86 handles --pid=2264:

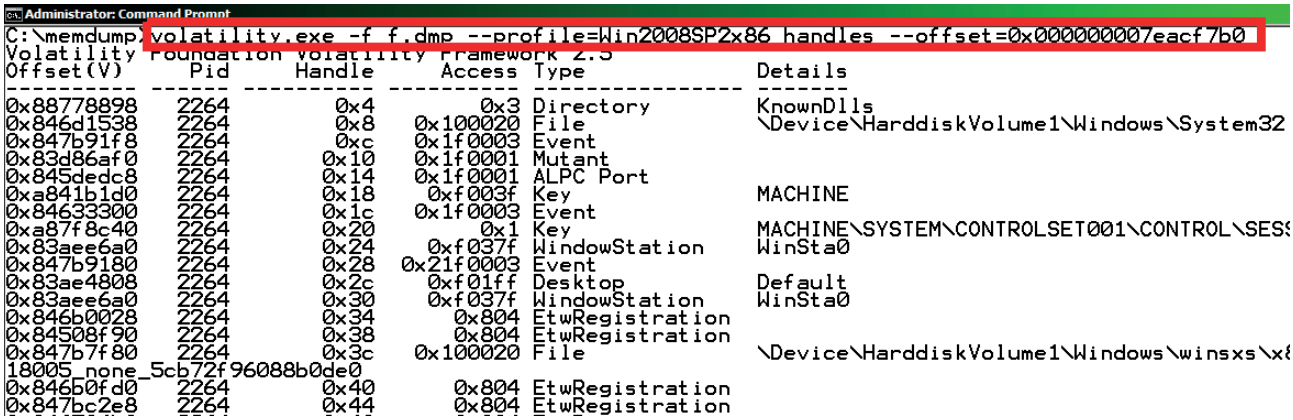


74. ábra

Információk összegyűjtése volatility-vel

Forrás: A szerző szerkesztése

Ilyenkor a --offset= kapcsoló az, amit használni kell. Az offsetet, illetve a pid-et az előbb használt pslist vagy psscan parancsok segítségével tudtuk meg, ez az első oszlop mindkét esetben. Például: volatility.exe -f f.dmp --profile=Win2008SP2x86 handles --offset=0x000000007eacf7b0



75. ábra

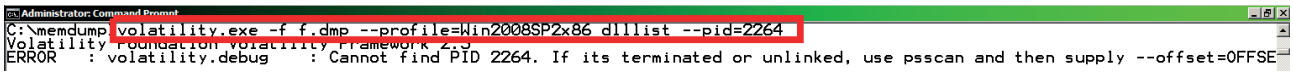
Az –offset= kapcsoló használata

Forrás: A szerző szerkesztése

9.4.1.6. Processek által használt dll-ek megtalálása

A processek által használt dll-ekből több hasznos következtetést is levonhatunk. Mit csinál az adott process (dll-ek általában pár cél megvalósítására tartalmaznak függvényeket például Ws2_32 az alacsony szintű hálózat kezelés, api32 registry kezelés, stb.). A parancs, amit használni kell, a dlllist, és működése hasonló az előzőhöz. Ha csak kiadjuk a parancsot, az összes process összes dll-jét kilistázza. Ezért inkább megadjuk a --pid= kapcsolóval a PID-et, amire kíváncsiak vagyunk. Szintén, rejtett process

esetében ez nem működik, az én példámban volatility.exe -f f.dmp --profile=Win2008SP2x86 dlllist --pid=2264.

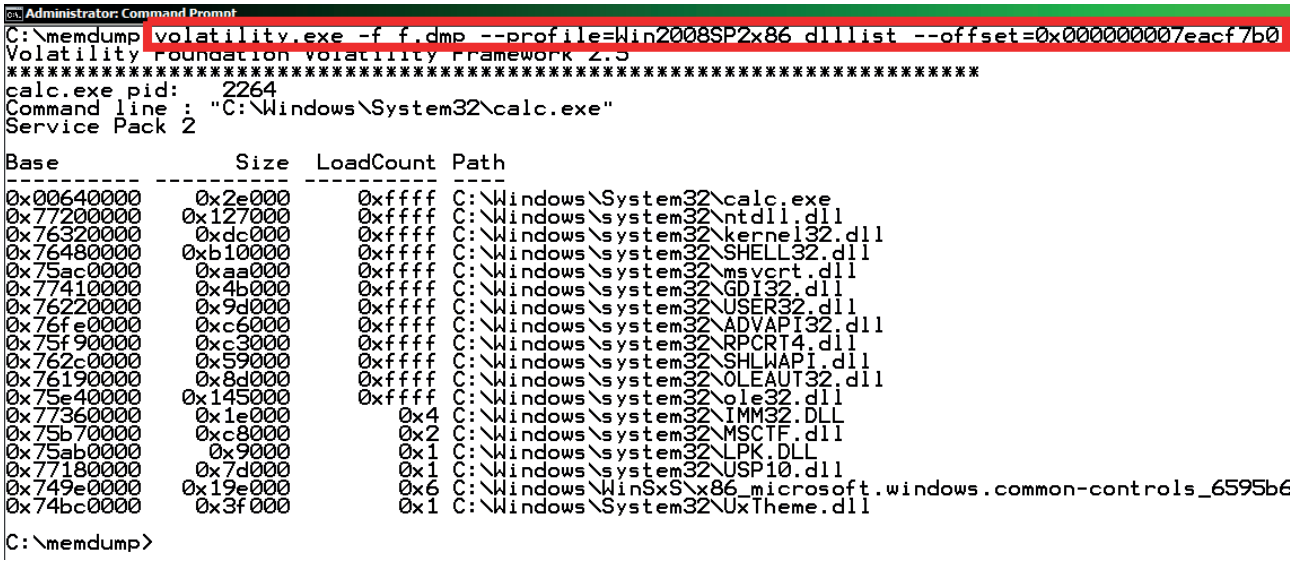


76. ábra

A dlllist parancs használata

Forrás: A szerző szerkesztése

Olyankor a --offset= kapcsolót kell használnunk, az én példámban volatility.exe -f f.dmp --profile=-Win2008SP2x86 dlllist --offset=0x000000007eacf7b0.



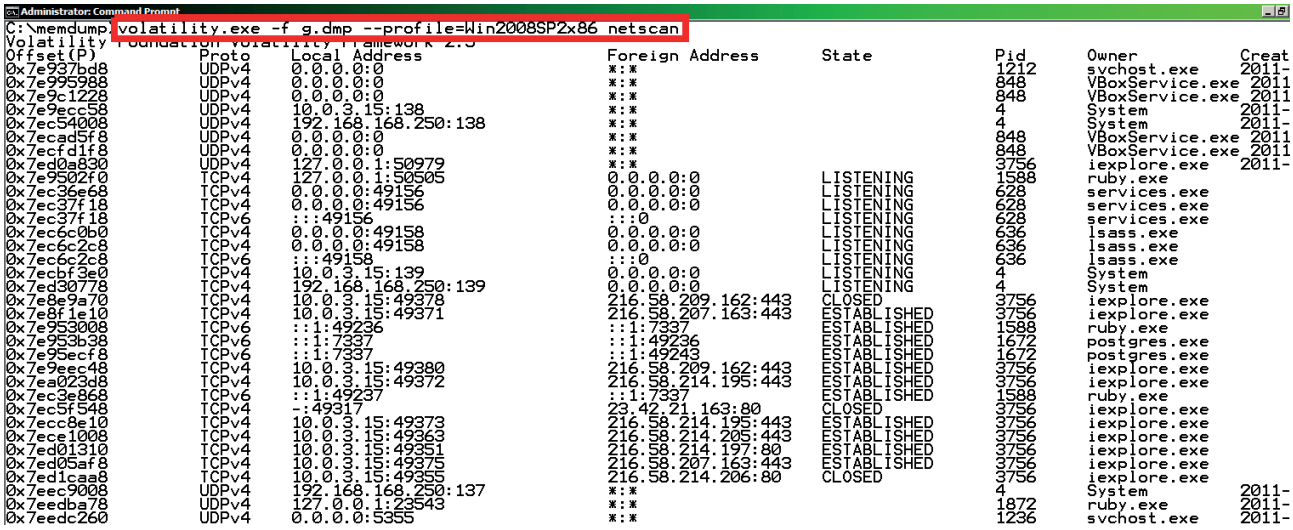
77. ábra

Az –offset= kapcsoló használata a dll-ek listázása során

Forrás: A szerző szerkesztése

9.4.1.7. A hálózati kapcsolatok kilistázása

A hálózati kapcsolatokból képet kaphatunk arról, ha egy gép például valamilyen botnet tagja volt, vagy kapcsolatot tart a Command and Conquer (CC) szerverrel. A hálózati kapcsolatokat más-más operációs rendszerek esetében máshogyan listázzuk. A Windows xp-2003ig a conscan illetve conlist parancsokkal, 2008 / vista-tól pedig a netscan paranccsal volatility.exe -f g.dmp --profile=Win2008SP2x86 netscan.

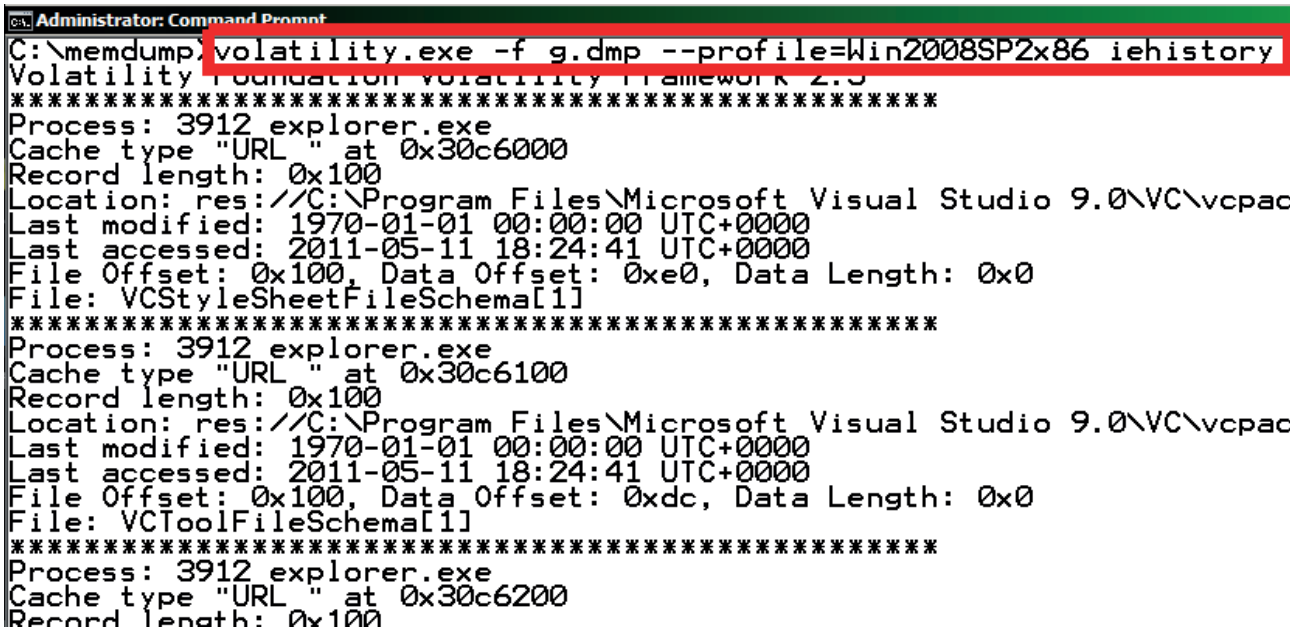


78. ábra

A hálózati kapcsolatok listázása

Forrás: A szerző szerkesztése

A nyitott kapcsolatokon kívül kilistázható az internet explorer history-ja is. Ezt az iehistory paranccsal tehetjük meg volatility.exe -f g.dmp --profile=Win2008SP2x86 iehistory.



79. ábra

Az internet explorer history listázása

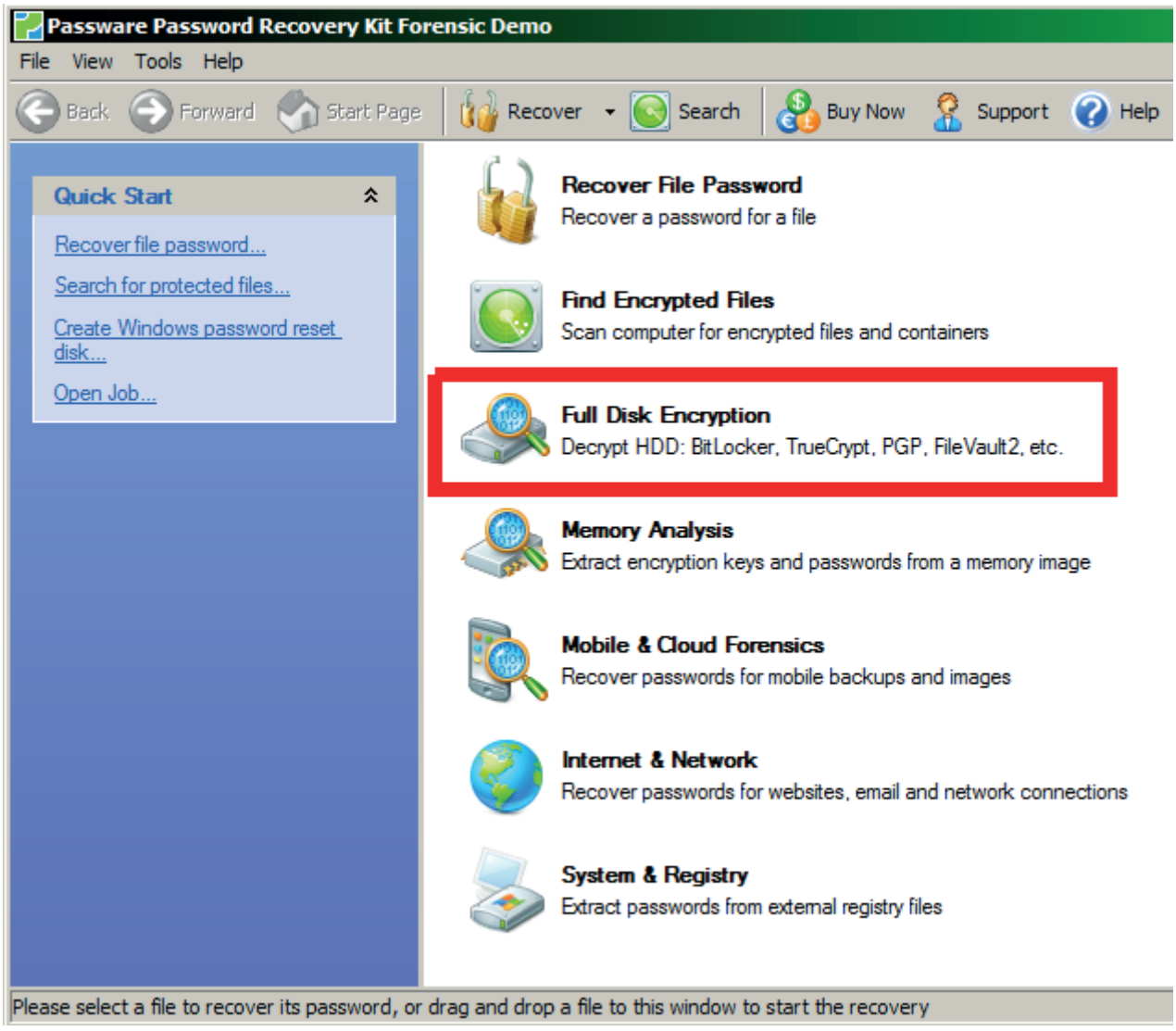
Forrás: A szerző szerkesztése

9.3.2. Lostpassword

A lostpassword kit egy példa a neten található számos jelszókiszedő framework-re. Sajnos nem ingyenes, mint ahogy a legtöbb ilyen alkalmazás sem. Demó verzió azonban letölthető és könnyen kipróbálható.

9.4.2.1. Truecrypttel (veracrypttel) titkosított disk kibontása

Indítsuk el az alkalmazást, és válasszuk a „Full disk encryption” parancsot.

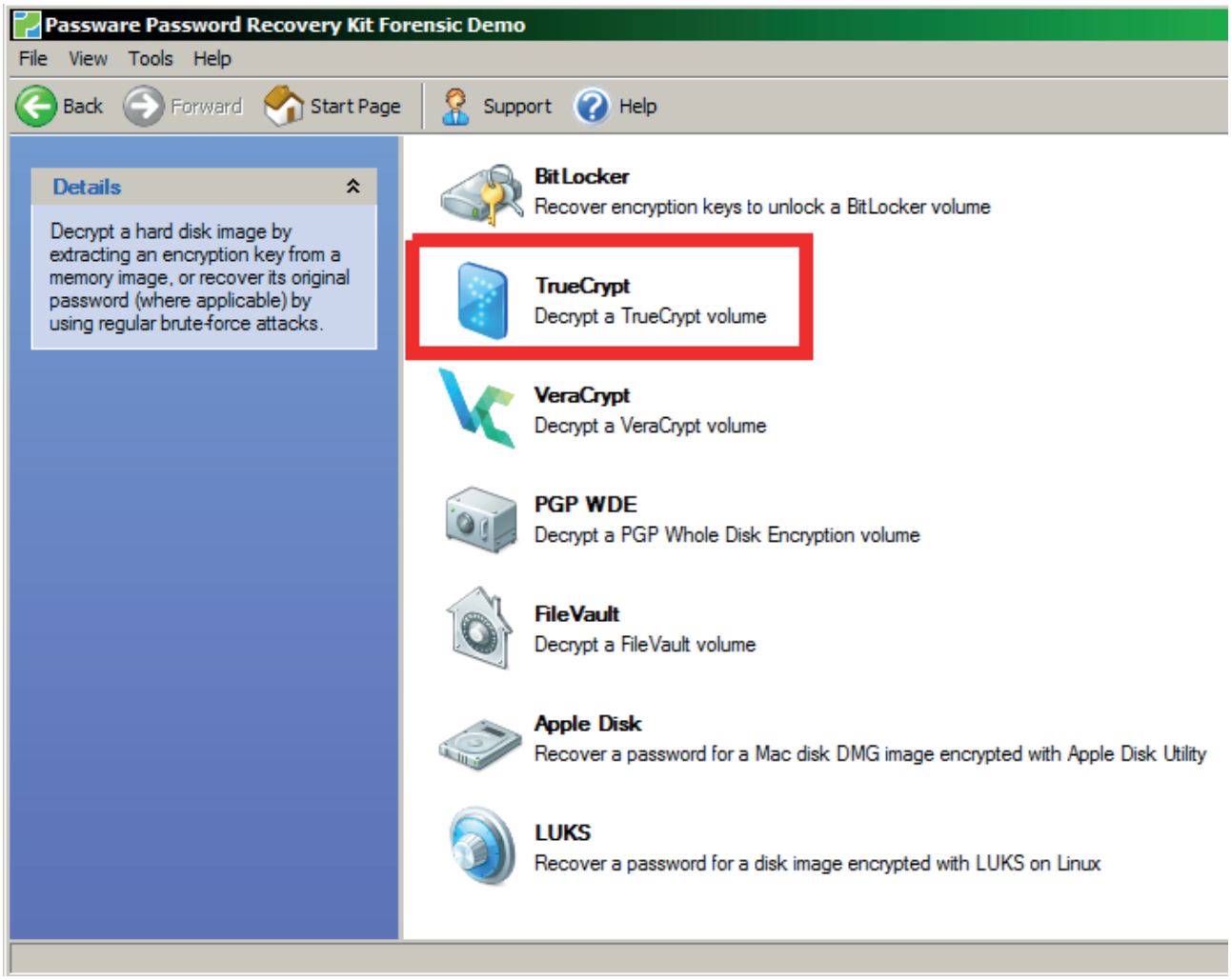


80. ábra

A Truecrypt alkalmazás indítása

Forrás: A szerző szerkesztése

A különböző titkosítási módok közül válasszuk a megfelelőt, nekem ez most a truecrypt.

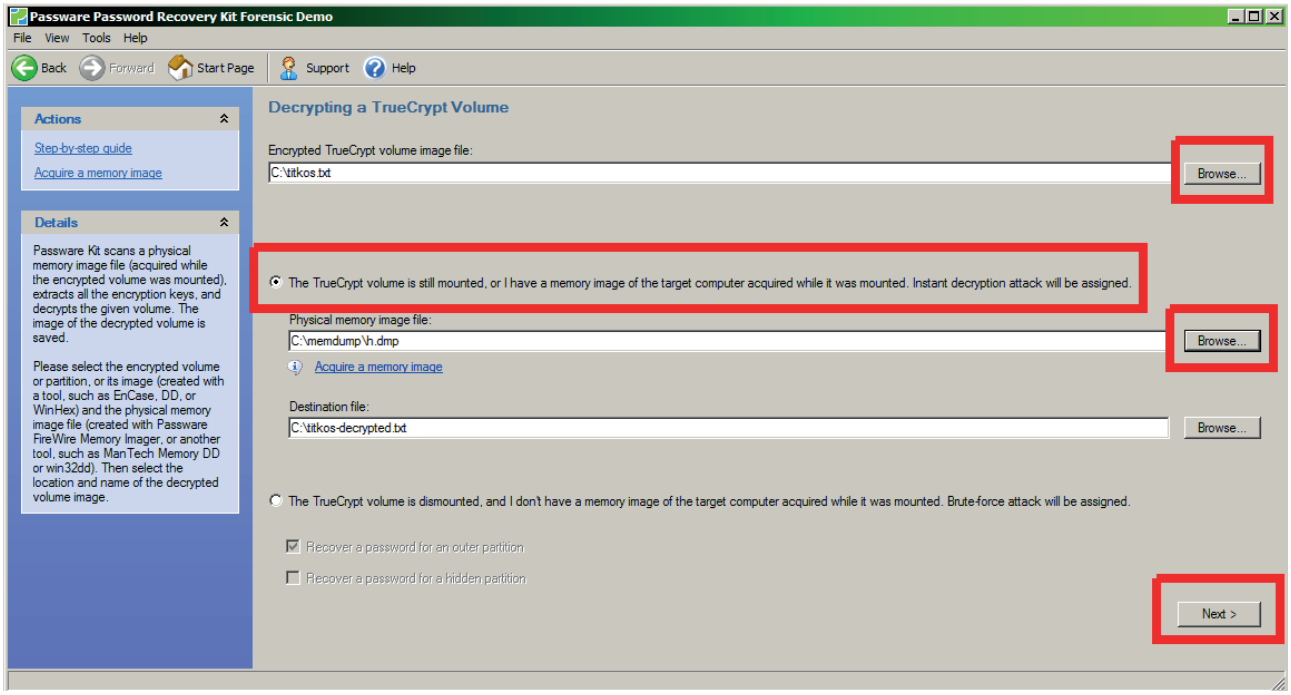


81. ábra

A megfelelő titkosítási mód kiválasztása

Forrás: A szerző szerkesztése

Adjuk meg a titkosított kötetet, illetve a memóriaimage-fájlt, majd kattintsunk a next gombra.

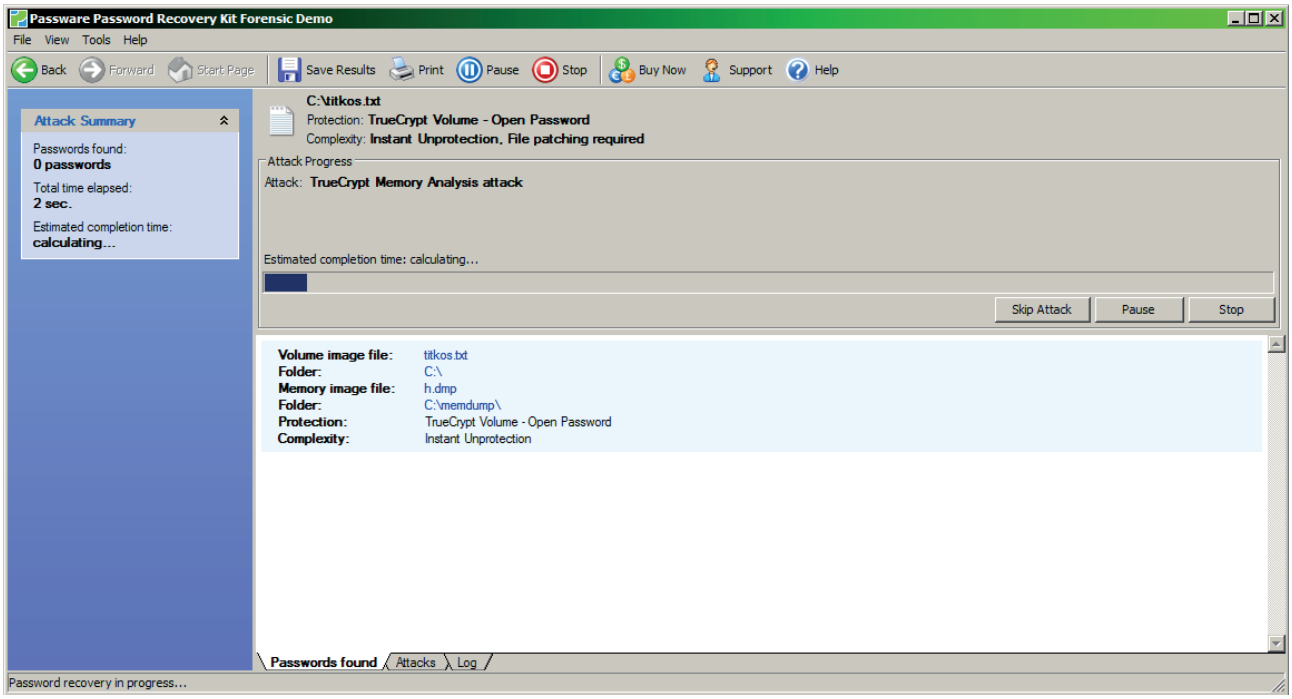


82. ábra

A titkosított kötet és a memóriaimage-fájl megadása

Forrás: A szerző szerkesztése

A decryptálás elindul, ki kell várni, amíg elkészül.

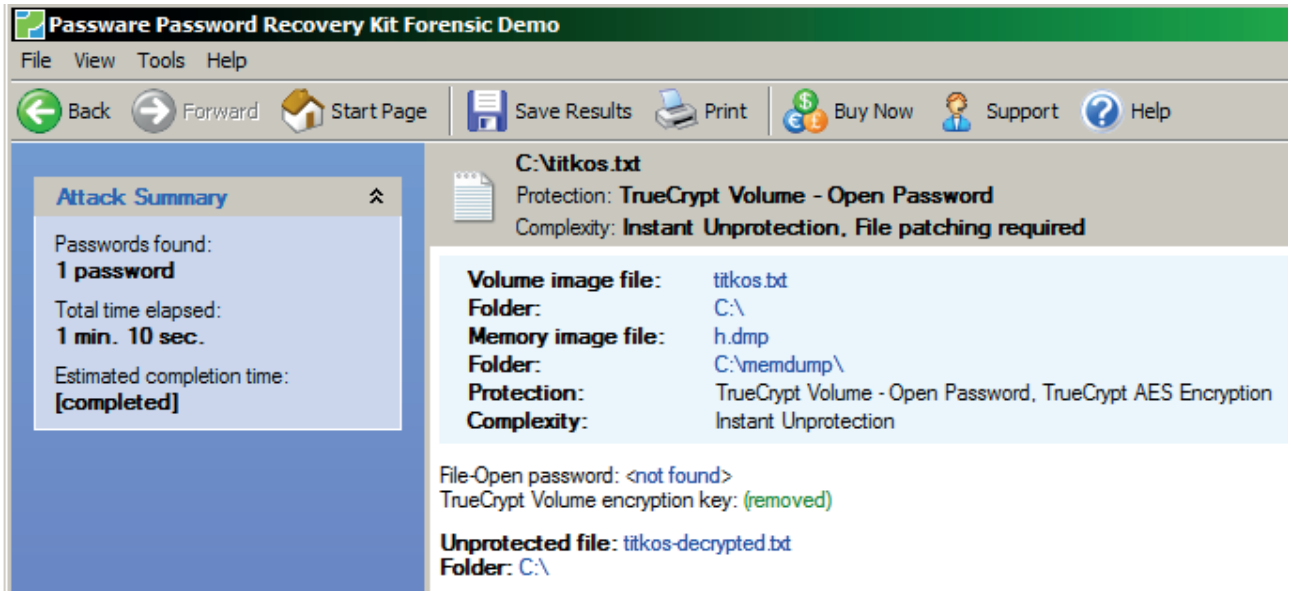


83. ábra

A decryptálás folyamata

Forrás: A szerző szerkesztése

A titkosítás eltávolítása után egy új fájlt kapunk, -decrypted szöveg van a neve végére fűzve.

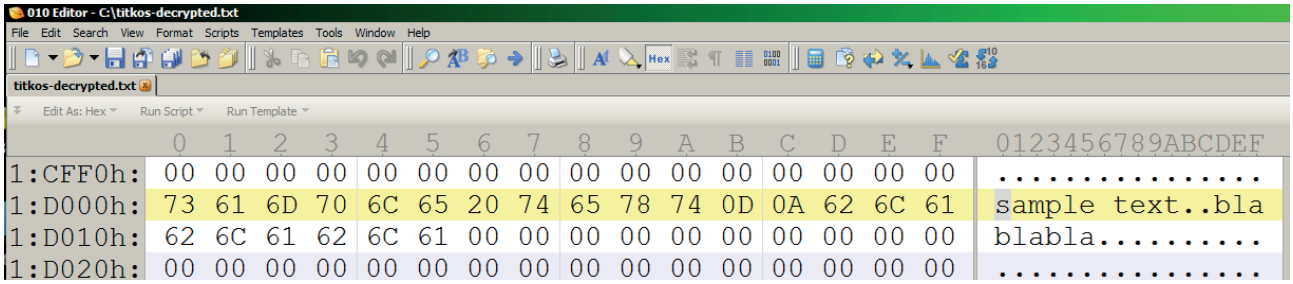


84. ábra

A titkosítás eltávolítása utána kapott új fájl

Forrás: A szerző szerkesztése

Ha ezt megnyitunk, egy partíciót találunk benne.



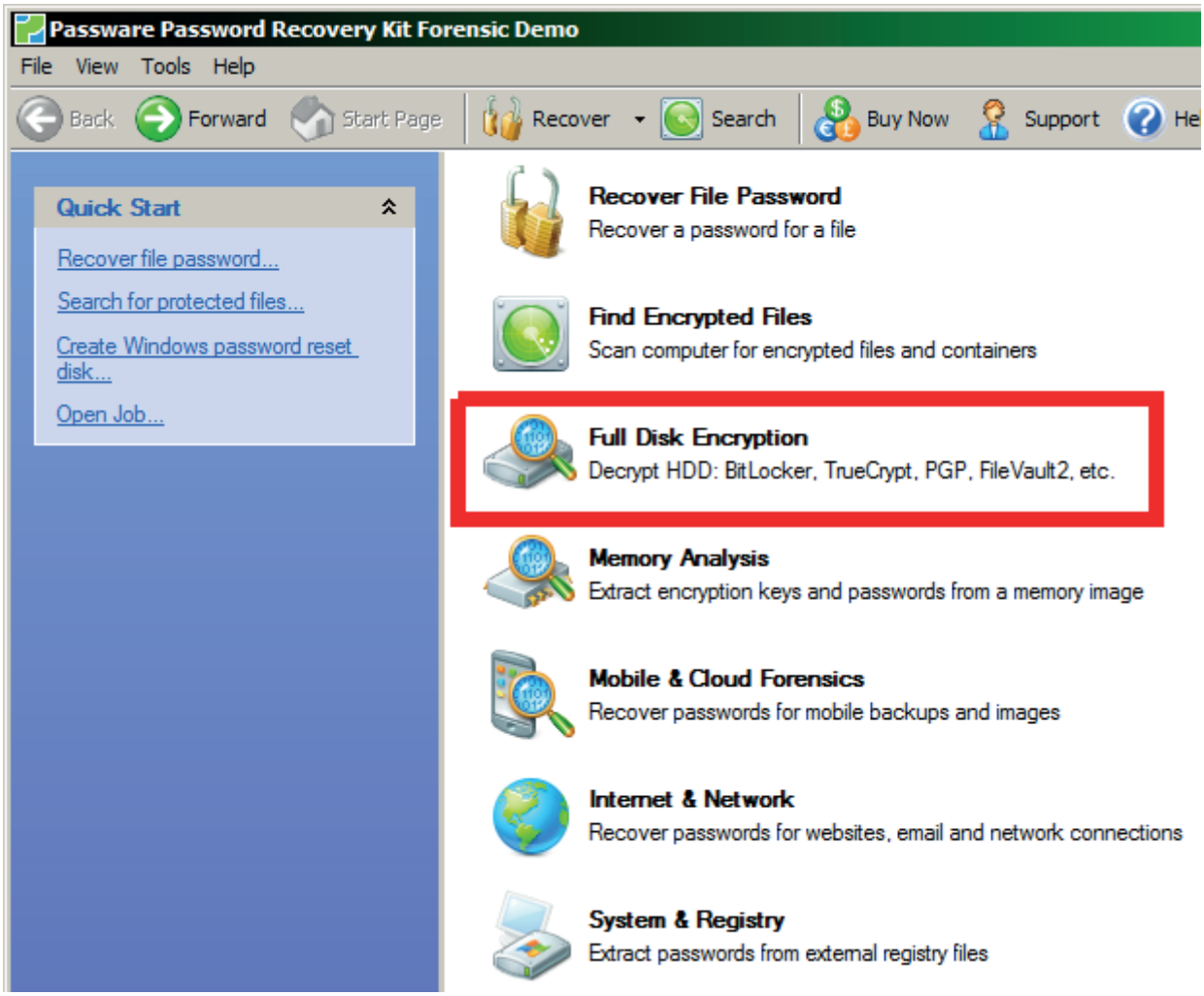
85. ábra

Az új fájlban található partíció

Forrás: A szerző szerkesztése

9.4.2.2. A bitlockerrel titkosított disk kibontása

A bitlockerrel titkosított disk kibontása nagyon hasonló a truecrypttel titkosított disk kibontásához. Indítsuk el az alkalmazást, és válasszuk a „Full disk encryption” parancsot.

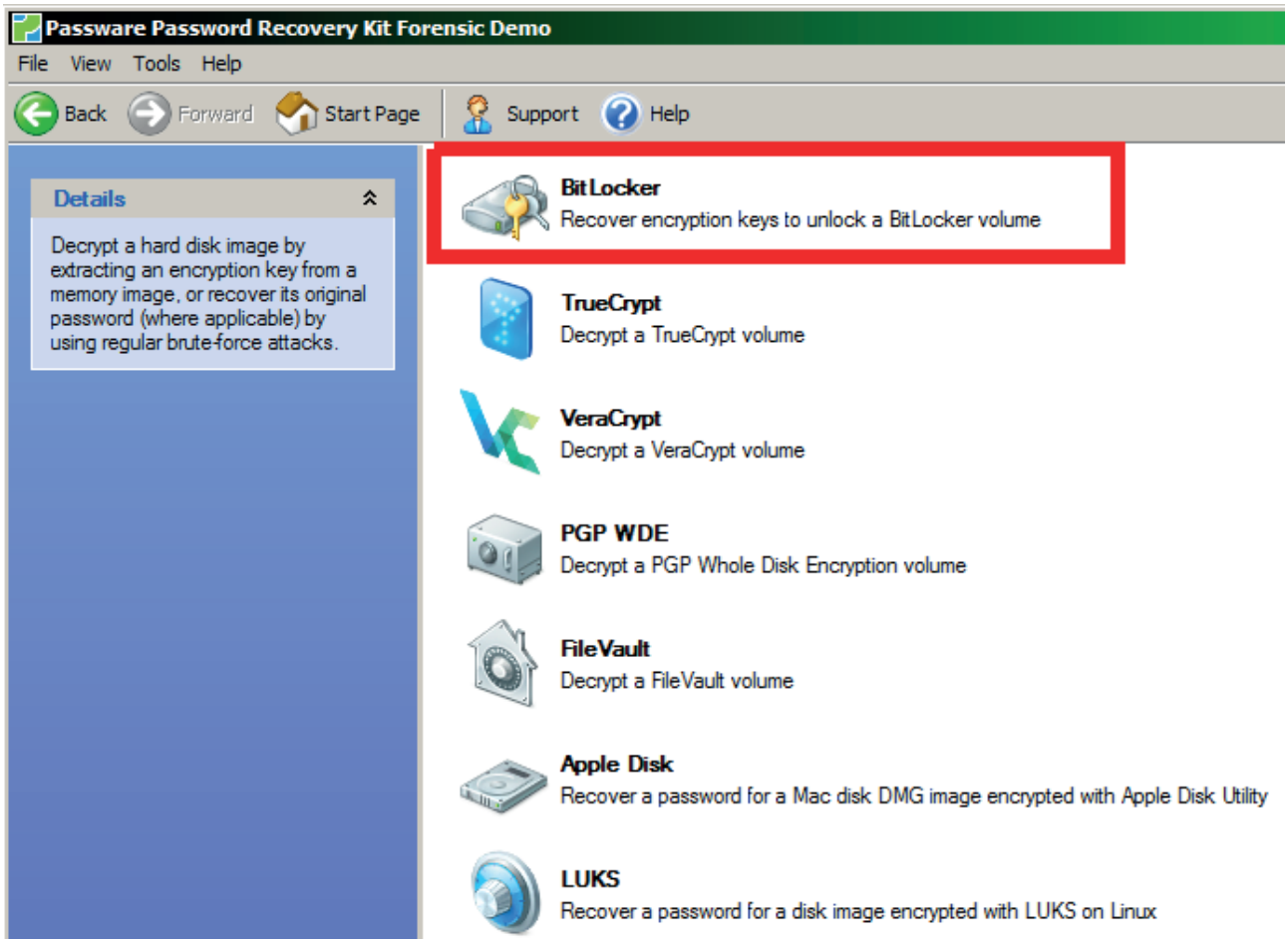


86. ábra

A bitlocker alkalmazás elindítása

Forrás: A szerző szerkesztése

A különböző titkosítási módok közül válasszuk a megfelelőt, nekem ez most a Bitlocker.

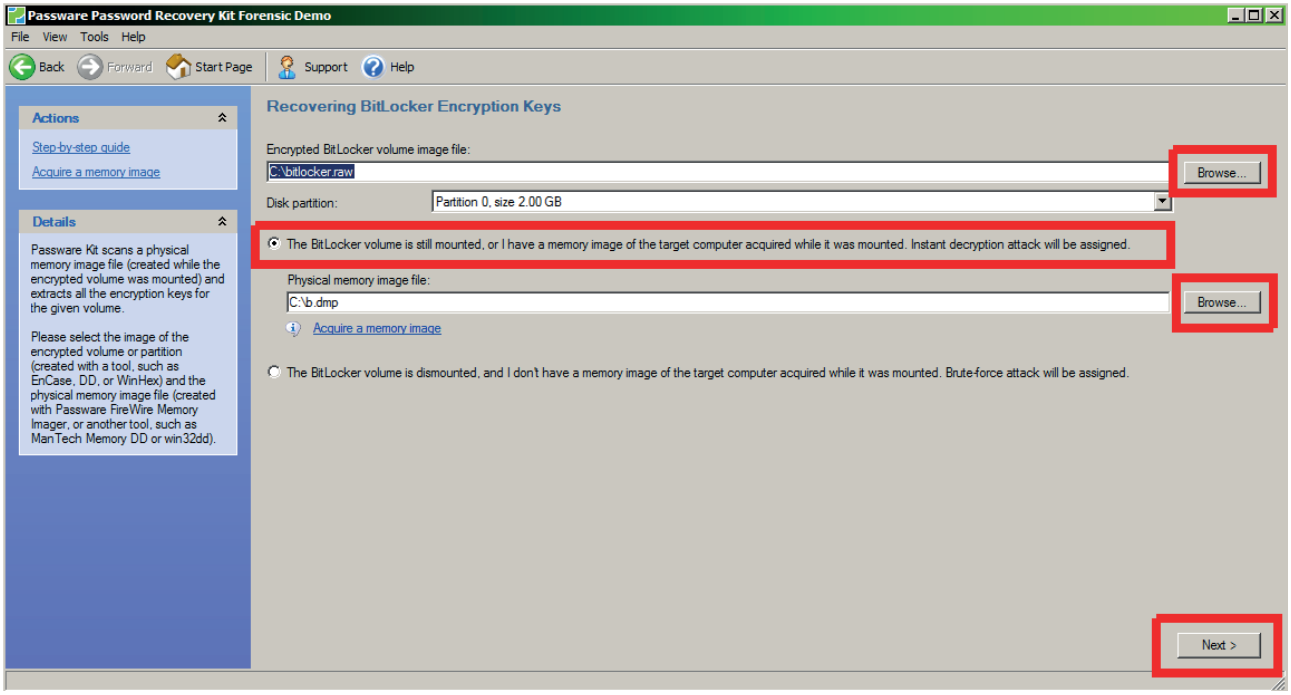


87. ábra

A megfelelő titkosítási mód kiválasztása

Forrás: A szerző szerkesztése

Adjuk meg a titkosított kötetet, illetve a memóriaimage-fájlt, majd kattintsunk a next gombra.

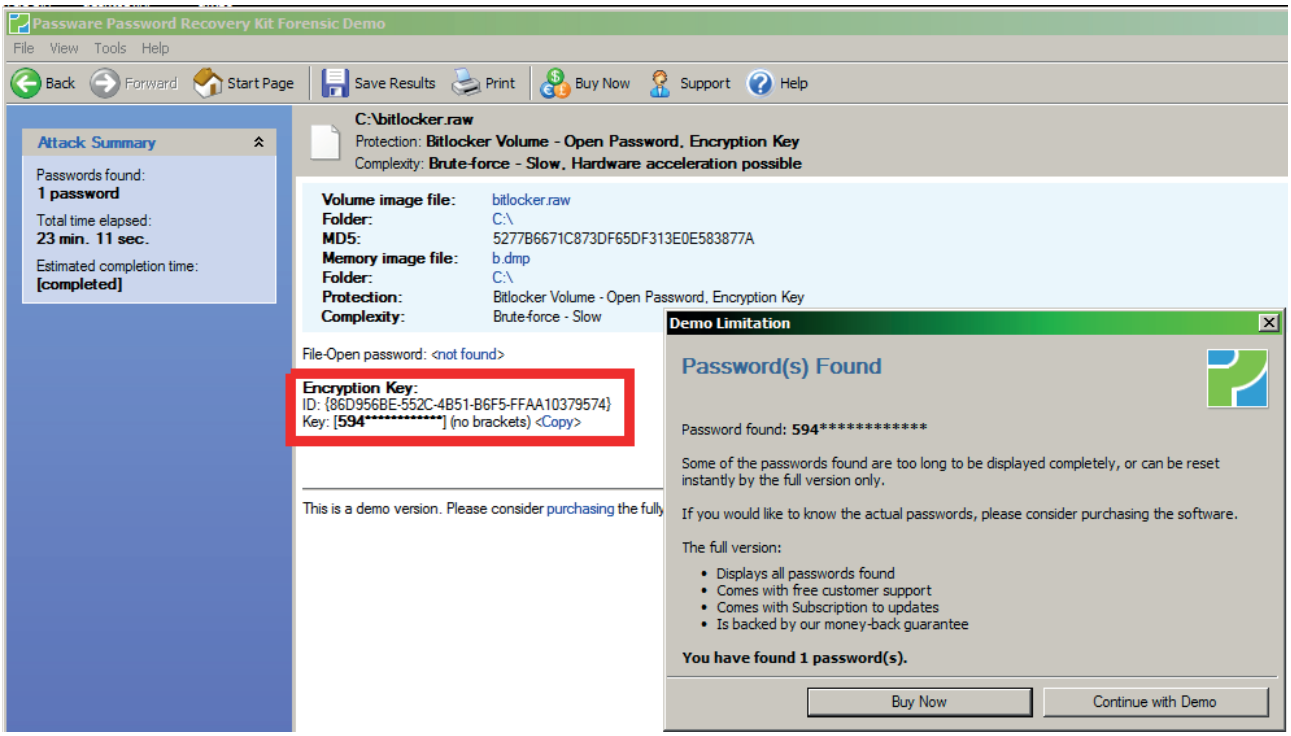


88. ábra

A titkosított kötet és a memóriaimage-fájl megadása

Forrás: A szerző szerkesztése

A decryptálás elindul, ki kell várni, amíg elkészül.

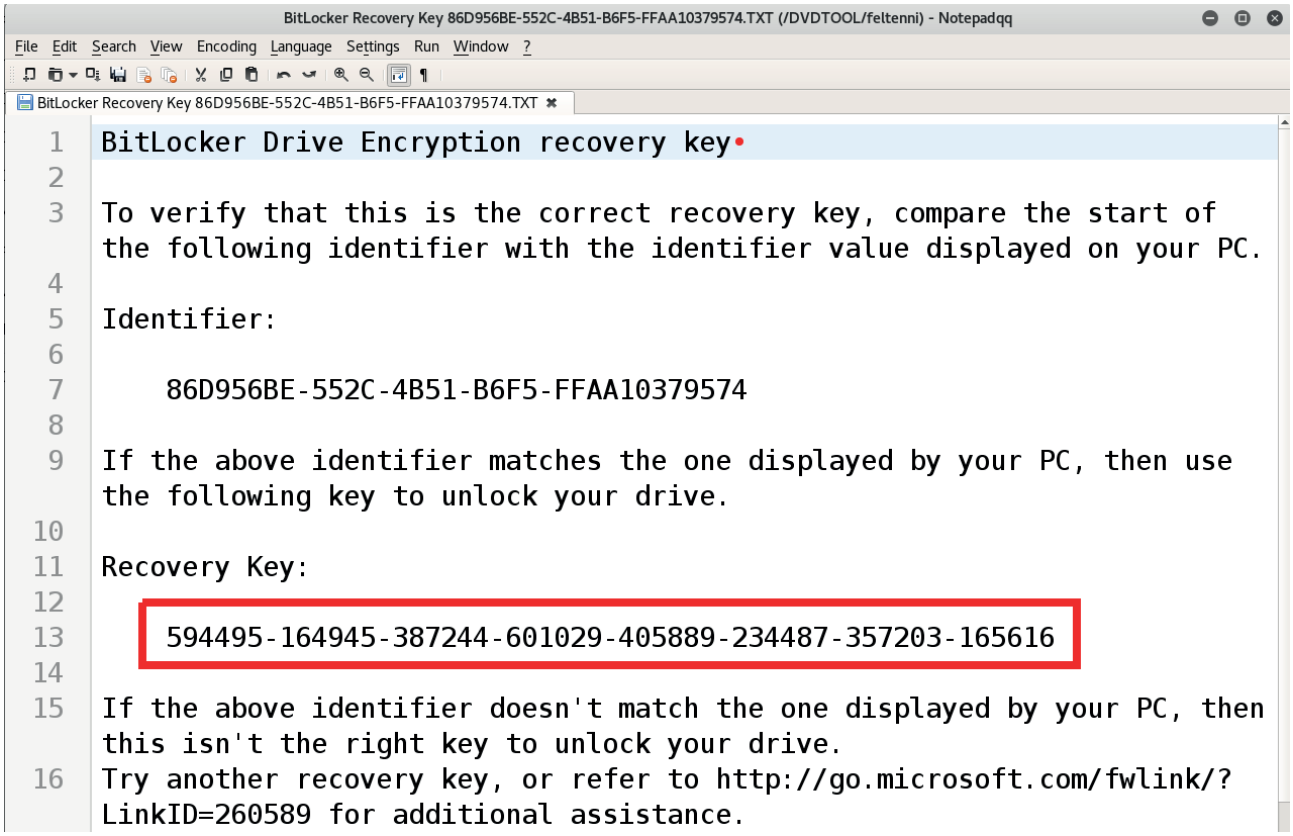


89. ábra

A decryptálás indítása

Forrás: A szerző szerkesztése

Sajnos a demó verzió nem mutatja meg a teljes kulcsot, csak az első 3 karaktert belőle, de mivel ez csak egy tesztkörnyezet volt, így megvan a bitlocker kibontó fájlja, így tudjuk ellenőrizni.



90. ábra

A bitlocker kibontó fájlja

Forrás: A szerző szerkesztése

9.4. A diskimage vizsgálata

Miután lefoglalták a disket, a következő lépés ennek a vizsgálata. Ebben a részben a fájlrendszerekről, illetve a törölt fájlok visszaállításáról, a software reference libraryk használatáról és hasonló dolgokról lesz szó. Az egyes hasznos információforrásokat (mint e-mailtartalmak, browser history, logok, registry) külön részekben nézzük meg, bár nyilván azok is a disken találhatók.

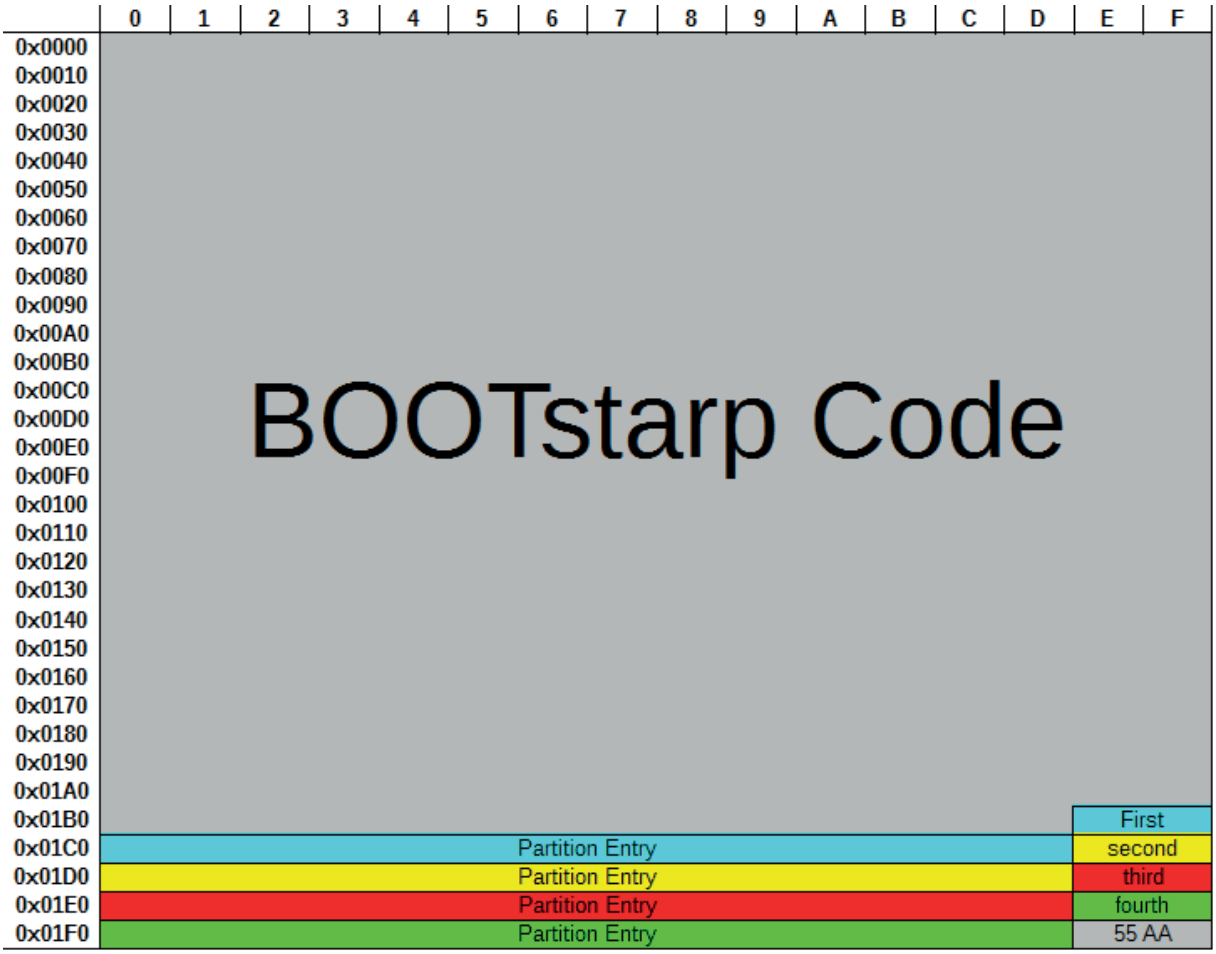
A merevlemez adatszervezése úgy néz ki, hogy mindent adategységekben, blokkokban vagy sectorokban (mindkét elnevezés elterjedt és szinonímaként használják) rögzít. Ez a legkisebb egység, amit a hardware ír vagy olvas. A legelterjedtebb az 512 bytos sectorméret, gyakorlatilag minden eszköz ezt használja. Állítólag léteznek 4096 bytos sectorméretttel dolgozó eszközök, de én eddig még nem találkoztam ilyennel.

9.4.1. Master Boot Record (MBR)

A Master Boot Record (MBR) mindig a disk nulladik sectorát (első 512=0x200 byteot) foglalja el. Miután a számítógép elindult, lefuttatta a Power On Self Testet (POST), illetve a BIOS kódot, ide adja át a vezérlést, az itt található úgynevezett „Bootstrap Code” kezd el futni. Ennek a kódnak a fő feladata a partíciók kezelése. Nem egyben akarjuk kezelni az egész disket, hanem több különálló egységként,

partíciónként (volumeonként). Az MBR-ben található kód feladata, hogy értelmezni tudja a partíciós bejegyzéseket, és a vezérlést továbbadja az első boot partíció Volume Boot Recordjának (VBR).

Rengeteg változata van, mint az összes itt megemlített, illetve megemlítendő adatstruktúrának. Nyilván nem cél, és nem is lehetséges mindegyiket bemutatni, ezért most a klasszikus MBR felépítést vázoljuk fel.



91. ábra

A Master Boot Record

Forrás: A szerző szerkesztése

Mint látható, az MBR a bootstrap kóddal indul. Utána találhatók a partíciós bejegyzések. A partíciós tábla végét egy magic érték jelöli 0x55 0xAA.

A legfontosabb itt található információk a partíciós bejegyzések. Maximum négy partíciós bejegyzést találhatunk (klasszikusan maximum 4 partíció hozható létre egy disken). Egy partíciós bejegyzés az alábbi módon néz ki:

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Bootable	start of the partition in CHS			Partition type	End of the partition in CHS			Start of partition in sectors (LBA notation)				Length of partition in sectors (LBA notation)			

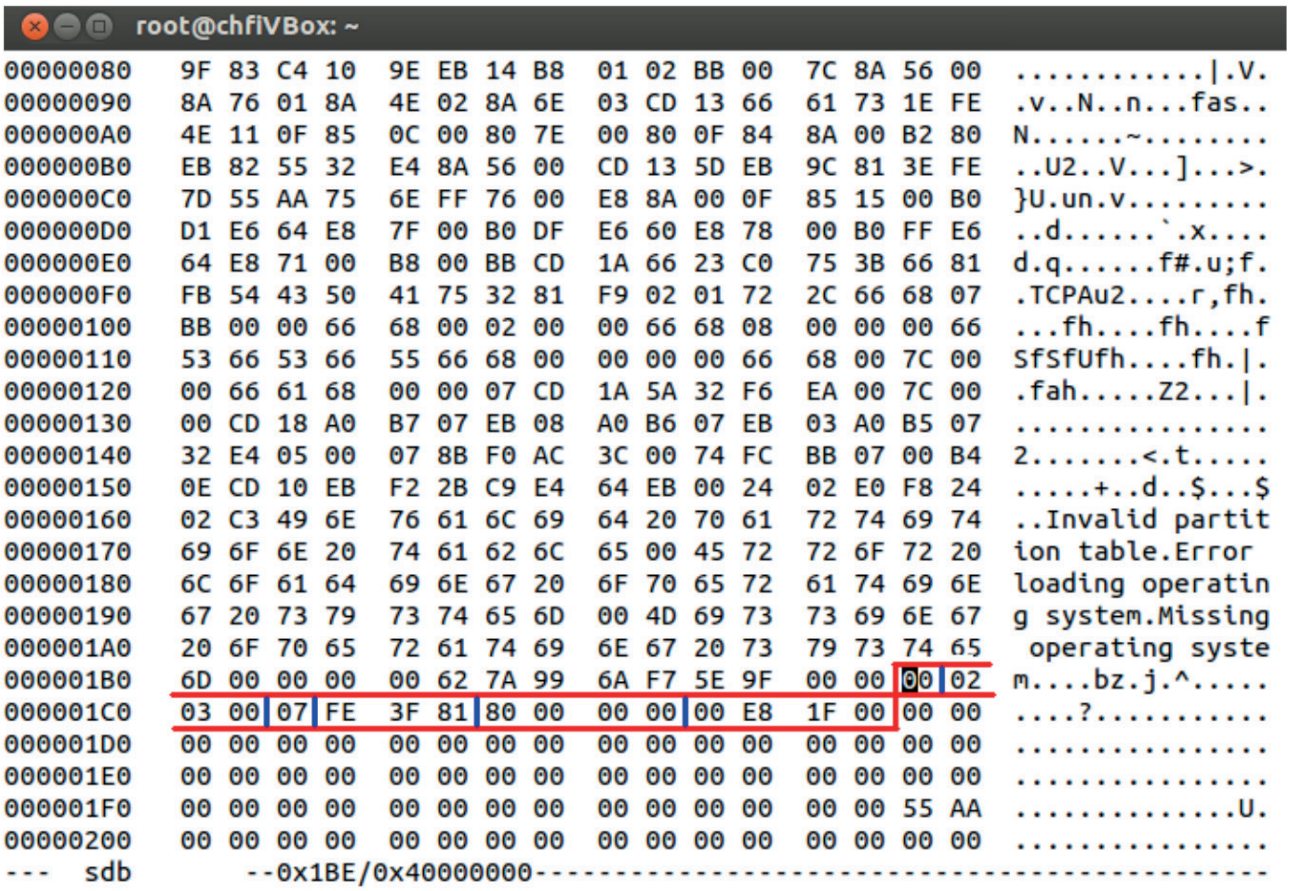
92. ábra

Partíciós bejegyzés

Forrás: A szerző szerkesztése

Az első byte jelenti, hogy bootolható-e a partíció, értéke 0x80 amennyiben igen, és 0x00, amennyiben nem. Az utána következő 3 byte a partíció kezdetét adja meg a régi CHS jelölési módban. Ezt ma már egyetlen rendszer sem veszi figyelembe. Elméletileg maximum 8 GB-os diskek kezelésére volt alkalmas. Majd a partíció típusa következik egy byteon, fontosabbak 0x07: NTFS, 0x06 MSDOS FAT, 0x42 Logical Volume Manager kezeli a partíciókat, 0x81 Linux, 0x83 linux újabb, 0x82 Linux SWAP, 0xEE GPT partíciós tábla van. Az utána következő 3 byte a partíció végét adja meg CHS jelölésben, ma már szintén nem használatos. Ezt követően látható 4 byteon a partíció kezdete LBA jelölésben (hányadik blokkon kezdődik a partíció), majd az utolsó 4 byte a partíció mérete blokkokban megadva.

Az itt található információt arra tudjuk használni, hogy megállapítsuk a partíció típusát, illetve a partíció kezdetét. Például:



93. ábra

A partíció típusának és kezdetének megállapítása

Forrás: A szerző szerkesztése

Az itt látható partíció 0x07 tehát NTFS, és a kezdete a 0x00000080 blokk vagyis a 0x80 * 0x200 = 0x10000 byte.

9.4.2. Guid Partition Table (GPT)

Az előbb ismertetett LBA partíciós bejegyzés maximum 2TB-os partícióig használható, ami manapság már kicsinek bizonyul, ezért született meg a GUID Partition Table GPT.

Amennyiben GTP-t használunk, akkor is megvan a hagyományos MBR, kompatibilitási okokból. Ez az úgynevezett Protective MBR, ez a maximális MBR-el leírható diskterületet foglaltnak mutatja, nehogy valamilyen eszköz azt higgye, hogy üres, lefoglalja, tönkretegye stb.

A GPT header rögtön az MBR után következő, tehát az első blokkban indul, és a következő 512=0x200 byteot foglalja el. Felépítése a következő:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x0000	Signature "EFI PART" 0x5452415020494645 little endian								Revision, 0x00000100				Header size in little endian			
0x0010	CRC32 of header with this field zeroed during calculation				Reserved; must be zero				Location of this header copy in blocks							
0x0020	location of the other header copy in blocks								First usable LBA for partitions (primary partition table last LBA + 1)							
0x0030	Last usable LBA (secondary partition table first LBA – 1)								Disk GUID (also referred as UUID on *NIX)							
0x0040	continuation of Disk GUID (also referred as UUID on *UNIX)								Starting LBA of array of partition entries (always 2 in primary copy)							
0x0050	Number of partition entries in array				Size of a single partition entry (usually 0x80 = 128)				CRC32 of partition array				Reserved, filled with 0			
0x0060	Reserved, filled with 0															
0x0070																
0x0080																
0x0090																
0x00A0																
0x00B0																
0x00C0																
0x00D0																
0x00E0																
0x00F0																
0x0100																
0x0110																
0x0120																
0x0130																
0x0140																
0x0150																
0x0160																
0x0170																
0x0180																
0x0190																
0x01A0																
0x01B0																
0x01C0																
0x01D0																
0x01E0																
0x01F0																

94. ábra

A GPT header felépítése

Forrás: A szerző szerkesztése

Innen nekünk a 0x48 byteon található Starting of LBA az érdekes. Ez adja meg, hogy hol találjuk a partíciódefiníciókat.

```
root@ubuntu: ~
00000200   45 46 49 20  50 41 52 54  00 00 01 00  5C 00 00 00  EFI PART....\...
00000210   A5 5B E5 C9  00 00 00 00  01 00 00 00  00 00 00 00  .[..............
00000220   FF FF 3F 00  00 00 00 00  22 00 00 00  00 00 00 00  ..?.....".......
00000230   DE FF 3F 00  00 00 00 00  8E A2 F4 FC  45 29 65 45  ..?.........E)eE
00000240   BA 56 29 8D  F9 7F AC 0B  02 00 00 00  00 00 00 00  .V).............
00000250   80 00 00 00  80 00 00 00  58 F4 6C A9  00 00 00 00  ........X.l.....
00000260   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00000270   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00000280   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00000290   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000002A0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000002B0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000002C0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000002D0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000002E0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000002F0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00000300   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00000310   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00000320   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00000330   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00000340   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00000350   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00000360   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00000370   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00000380   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
00000390   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000003A0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000003B0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000003C0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000003D0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000003E0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000003F0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
---  sdb       --0x200/0x80000000----------------------------------------------
```

95. ábra

Partíciódefiníciók helyei

Forrás: A szerző szerkesztése

Itt azt látjuk, hogy a partícióleírások a 0x02 pozíción, vagyis a második blockon, tehát a 0x02 * 0x200 = 0x400 byteon kezdődnek.

A partícióheader felépítése a következő:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x0000	Partition type GUID															
0x0010	Unique partition GUID															
0x0020	First LBA								Last LBA (inclusive)							
0x0030	Attribute flags															
0x0040	Partition name (UTF-16LE)															
0x0050																
0x0060																
0x0070																

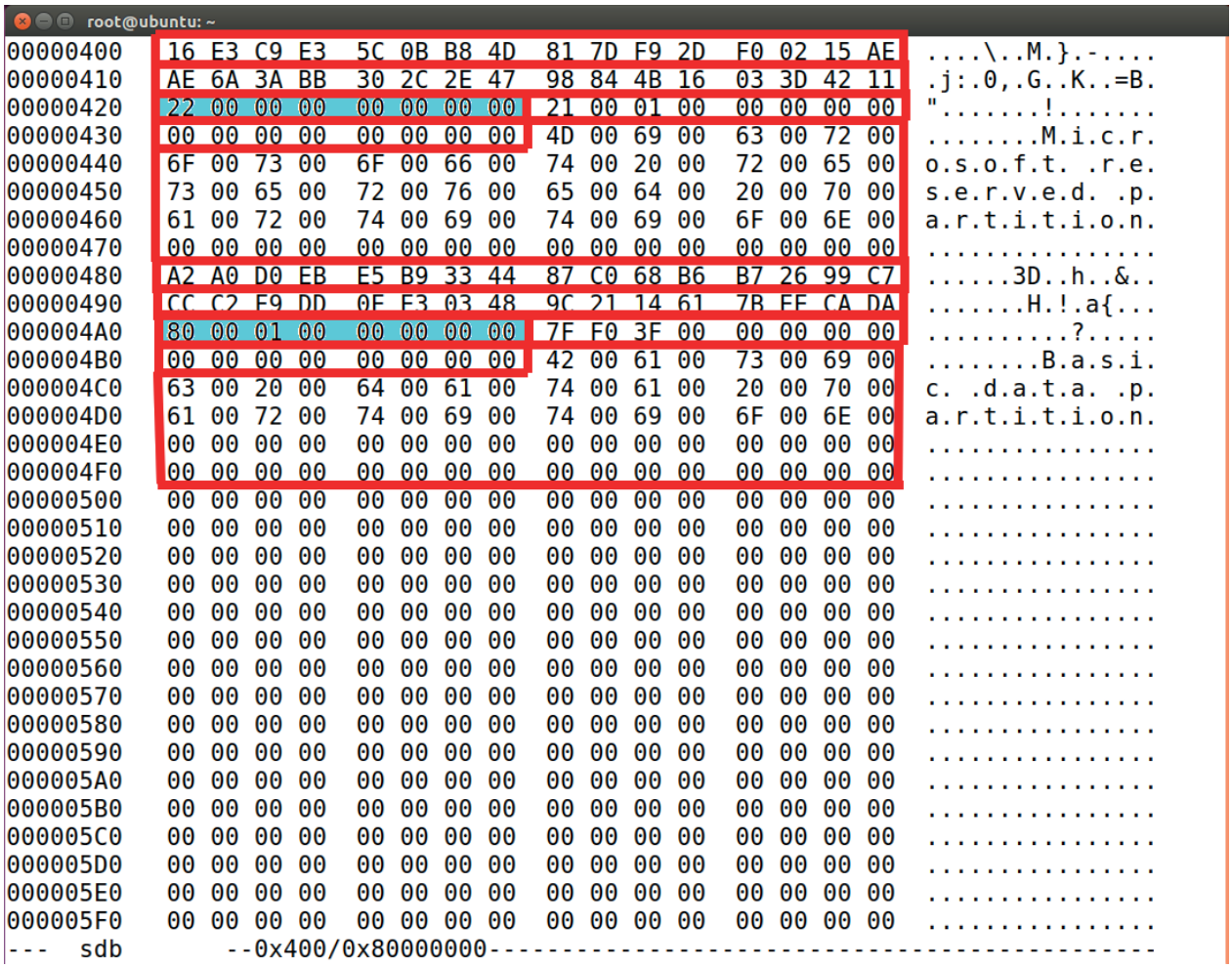
96. ábra

A partícióheader felépítése

Forrás: A szerző szerkesztése

Innen nekünk leginkább az egyes partíciók kezdete az érdekes, illetve a partíció típusát azonosító GUID.

Nézzünk erre is egy példát:

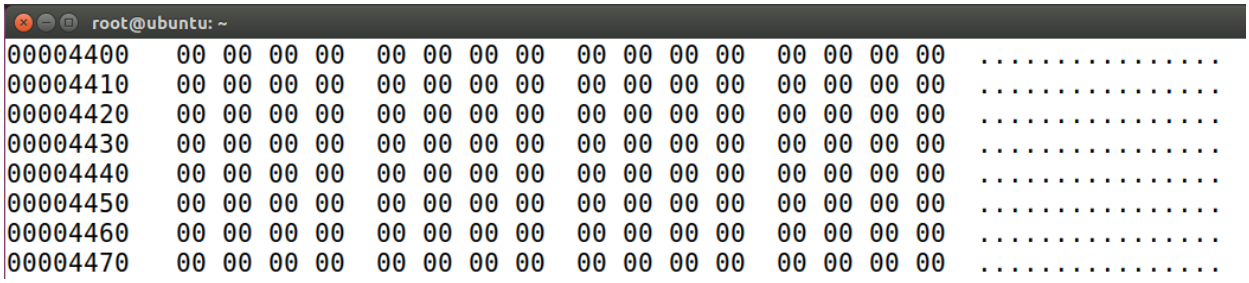


97. ábra

A partíciók kezdetére és típusára vonatkozó információk

Forrás: A szerző szerkesztése

Itt azt látjuk, hogy két partíció van, az első a 0x22 blokkon kezdődik, vagyis a 0x22 * 0x200 = 0x4400 byte-on. A második a 0x010080 blokkon kezdődik, tehát a 0x010080 * 0x200 = 0x02010000 byte-on. Ezek közül az én esetemben csak a második tartalmaz adatot, az elsőt az operációs rendszer fenntartja magának.

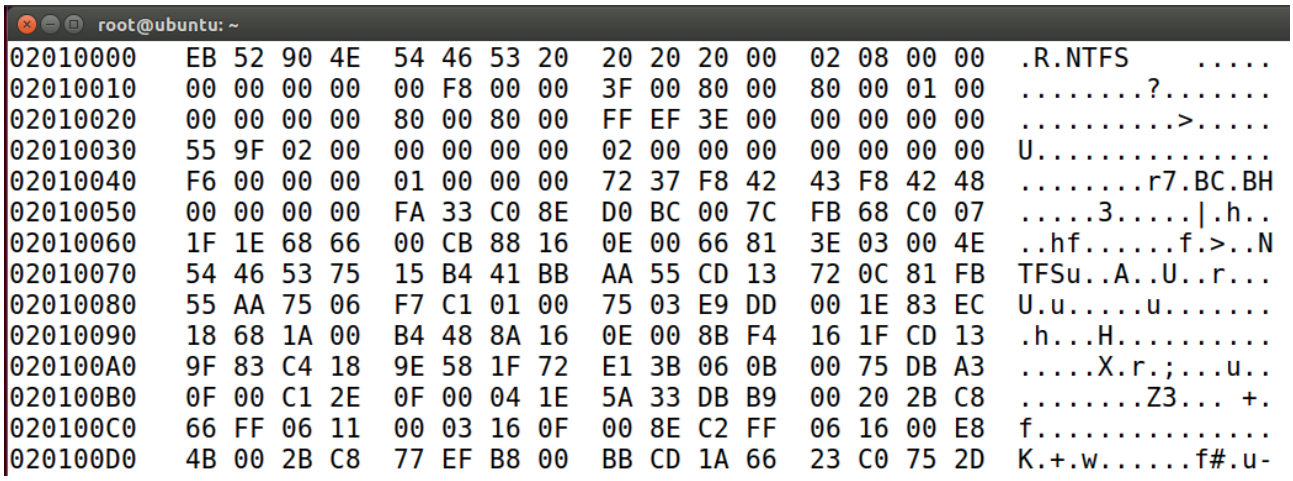


98. ábra

Az operációs rendszer által fenntartott hely

Forrás: A szerző szerkesztése

A második egy NTFS partíció.



99. ábra

NTFS partíció

Forrás: A szerző szerkesztése

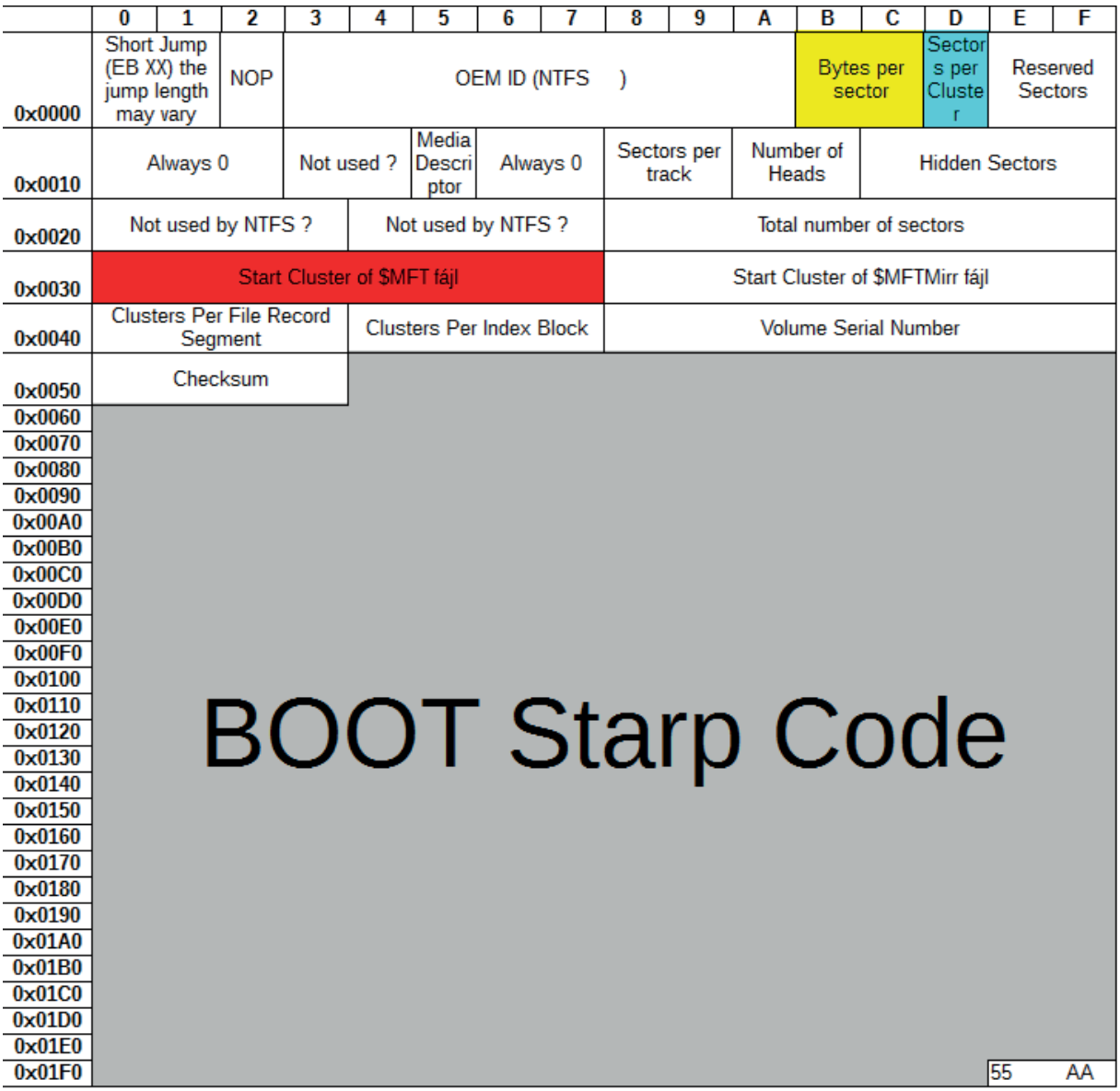
Most már akár klasszikus MBR, akár GPT van az adott disken, képesek vagyunk megtalálni az egyes partíciók (volumeok) kezdetét. Következő lépés a partíciók vizsgálata.

9.4.3. Volume Boot Record (VBR)

Minden partíció az úgynezvezett Volume Boot Recorddal kezdődik. Ez szintén egy futtatható kódot tartalmaz, illetve a partíción található filerendszer metaadatait. Ennek a kódnak a legfontosabb feladata, hogy olyan szinten értelmezni tudja a fájlrendszert, hogy megtalálja az első fájlt, amit el kell indítania, windows esetében ez az ntldr nevezetű alkalmazás. A Volume boot record felépítése függ attól, hogy milyen fájlrendszer található itt, de vannak közös pontok. Az első 3 byte egy shortjump és egy NOP utasítás placeholdernek. A short jump átugorja a partíció metainformációkat, és a kódon folytatja a futást. A metainformációs block mérete az, ami fájlrendszerek esetében különbözik.

9.4.4. NTFS fájlrendszer

Az NTFS fájlrendszer esetében a Volume Boot Record a következőképpen néz ki:



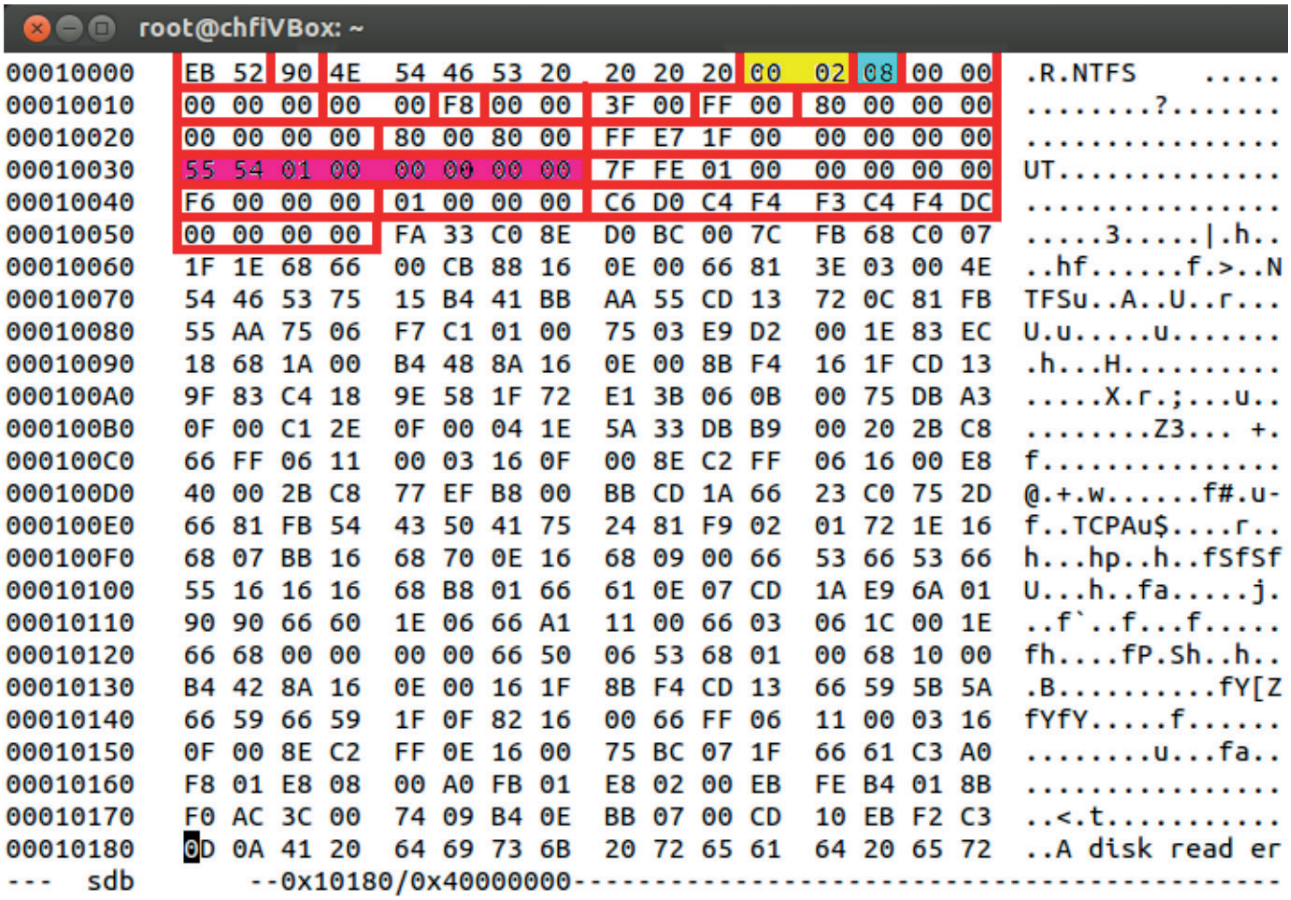
100. ábra

A Volume Boot Record az NTFS fájlrendszer esetében

Forrás: A szerző szerkesztése

Az itt található legfontosabb információk a következők: a blokkméret, ami általában 512=0x0200, majd a clusterméret blokkokban megadva, legtöbbször 0x08, ami az alapértelmezett 4096 byte-os clusterméretthez tartozik. Illetve a Master File Table (MFT) kezdő clustere. A Master File Table az a leíró, ami az összes többi fájlról tartalmazza a metainformációkat (például, hogy mikor hozták létre, mikor nyitották meg utoljára, mi a neve), illetve a fájl tartalmát leíró clusterláncra vonatkozókat.

Nézzünk ismét egy példát!



101. ábra

Master File Table

Forrás: A szerző szerkesztése

Innen a következő adatok a legfontosabbak nekünk:

- block (sector) méret (bár ezt eddig is tudtuk, másképpen nem találtunk ide): 0x0200 = 512;
- cluster méret: 0x08 block = 0x08 * 0x0200 = 0x1000 = 4096 byte;
- MFT kezdő clustere: 0x015455.

Most már megkereshetjük a Master File Table elejét!

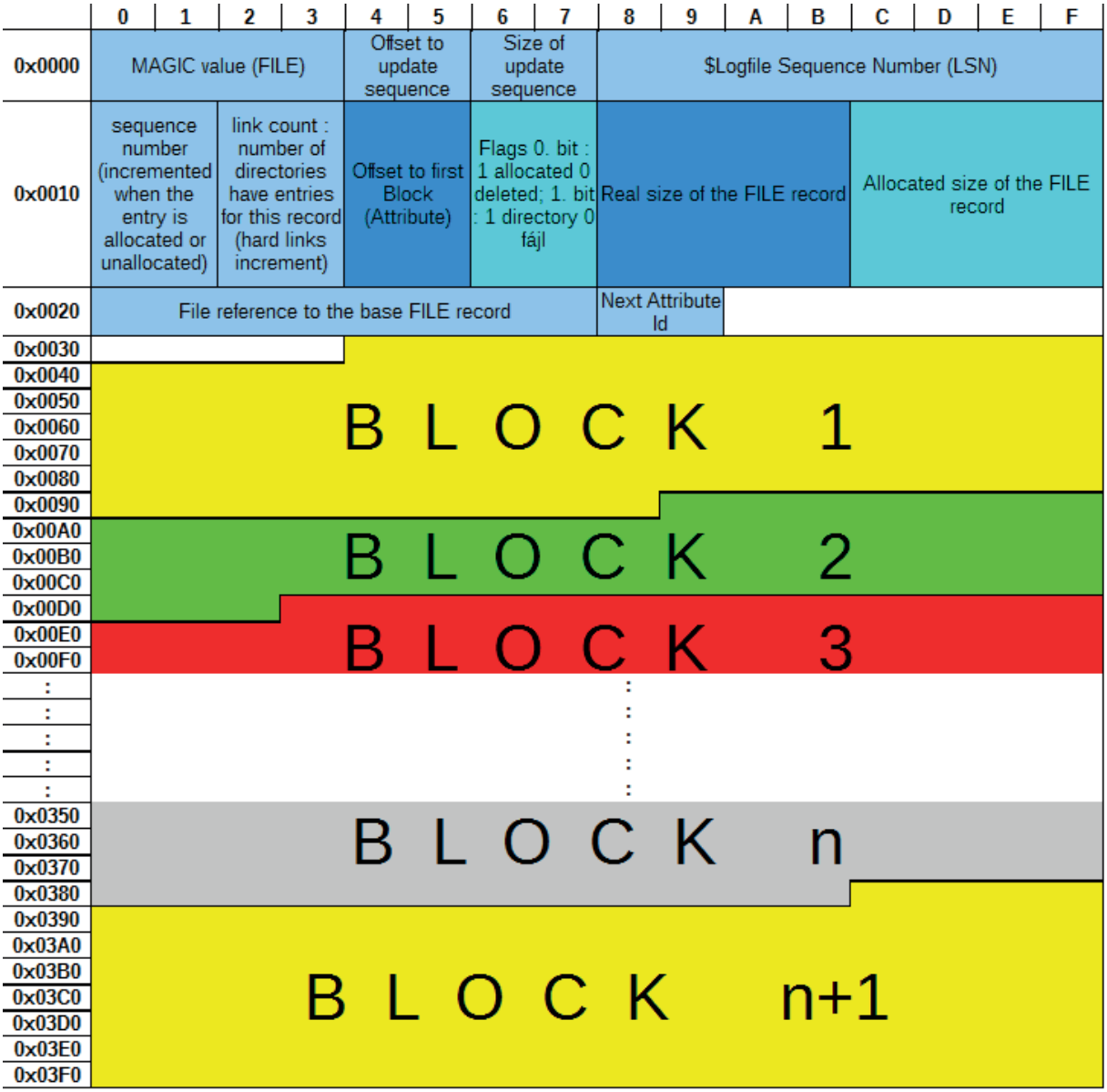
Tudjuk, hogy a 0x015455 clusteren van, és egy cluster mérete 0x1000 byte, tehát az MFT a Volume elejétől számítva a 0x015455 * 0x1000 = 0x15455000 byteon található.

Mivel a partíció a 0x10000 byte-on kezdődik, ezért az MFT kezdetének az abszolút pozíciója: 0x15455000 + 0x10000 = 0x15465000.

A Master File Table a következőképpen épül fel: a Master File Tableben minden fájlhoz tartozik egy bejegyzés, és egy bejegyzés 1024 byte-os, vagyis 0x0400 byte-os.

Az első általában 35 = 0x23 bejegyzés a rendszer számára fenntartott.

A bejegyzések blokkokra osztottak, mint az a következő ábrán látható:



102. ábra

Blokkokra osztott bejegyzések

Forrás: A szerző szerkesztése

Az MFT bejegyzés fejléce minden esetben azonos, és a FILE magic értékkel kezdődik. Itt a legfontosabb információk a következők:

- Offset to first blokk, ez a bejegyzés elejétől számítva megadja, hogy hányadik byte-on kezdődik az első blokk, innentől kezdve lépésenként tudjuk felépíteni.
- Flags: itt láthatjuk, hogy fájl vagy alkönyvtár-e a bejegyzés, illetve, hogy törölt-e vagy sem.

A blokkok felépítése attól függ, milyen fajta. Ezt egy szám határozza meg. A nekünk legfontosabb három típus a következő:

- standard information blokk, 0x10;
- filename blokk 0x30;
- data blokk 0x80.

Ezek a következőképpen épülnek fel:

9.4.4.1. Standard Information Block 0x10

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x0000	Attribute type (Standard Information10000000)				Length of this attribute entry including the header				Resident flag	Length of stream name	Offset to stream name		Flags		Attribute identifier	
0x0010	Length of data from the end of header				Offset to attribute content		Padding 00, if length stream name not 0 after it the stream name		Creation Time in windows 64 bit time format							
0x0020	Last Modification Time in windows 64 bit time format								Last Modification Time of the File Record in windows 64 bit time format							
0x0030	Last Access Time in windows 64 bit time format								DOS File Permissions (flags)				Maximum number of versions			
0x0040	Version number								Class ID				Owner ID			
0x0050	Security ID				Quota charged				Update Sequence Number (UCN)							

103. ábra

A Standard Information Block 0x10 felépítése

Forrás: A szerző szerkesztéser

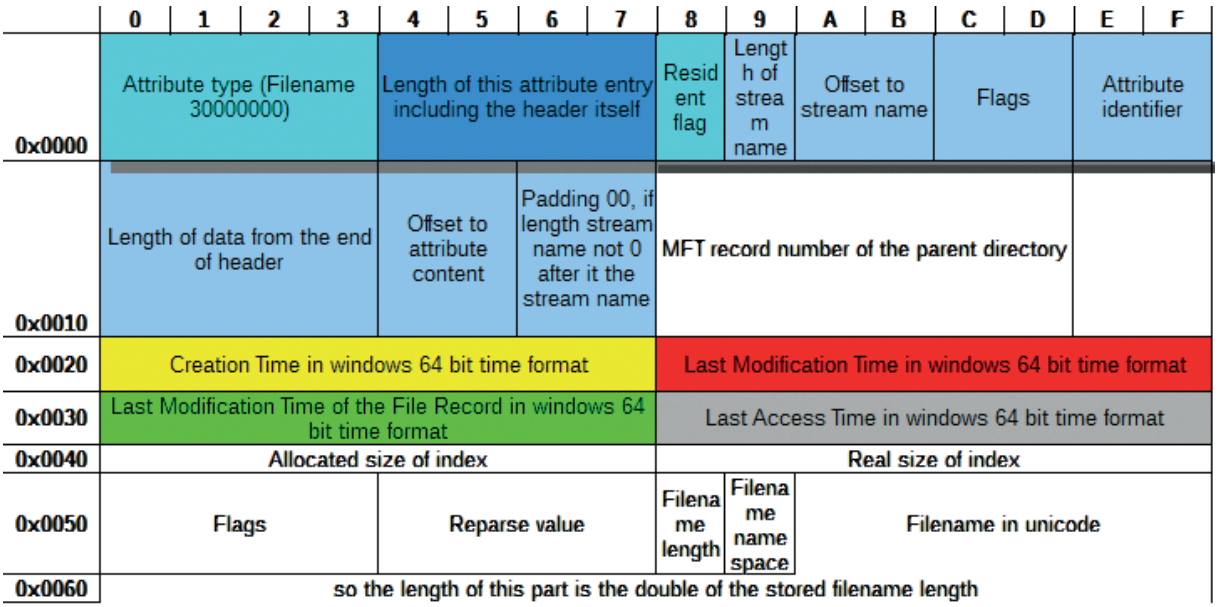
Az itt található legfontosabb információk az időre vonatkozók:

- creation time 64 bites windows időformátumban (1601 január 01. 00:00:00 óta eltelt 10^{-7} másodpercek száma) ezt C-vel szokták jelölni;
- last modification time a fájltartalomnak 64 bites windows időformátumban, ezt M-el szokták jelölni;
- last modification time az NTFS bejegyzésnek 64 bites windows időformátumban, ezt E-vel szokták jelölni;
- last access time 64 bites windows időformátumban, ezt A-val szokták jelölni.

Ezek együtt a CMEA idők.

9.4.4.2. Filename Block 0x30

Ebből a blokktípusból több is lehet. Ha a fájl neve hosszabb, mint a 8+3 karakteres DOS fájlnév, akkor mindenképpen két filename block lesz, az egyik a 8+3 karakteres rövid DOS fájl nevet tartalmazza (a ~-s név), míg a másik a teljes nevet.



104. ábra

A Filename Block 0x30 felépítése

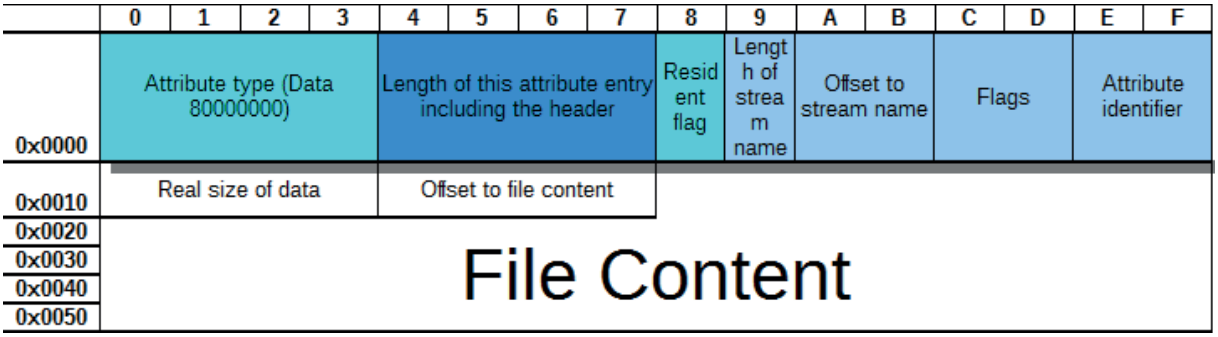
Forrás: A szerző szerkesztéser

Az itt található legfontosabb információk:

- filename length, a fájlnév hossza;
- filename: a fájlnév;
- creation time 64 bites windows időformátumban (1601 január 01. 00:00:00 óta eltelt 10^{-7} másodpercek száma), ezt C-vel szokták jelölni;
- last modification time a fájltartalomnak 64 bites windows időformátumban, ezt M-el szokták jelölni;
- last modification time az NTFS bejegyzésnek 64 bites windows időformátumban, ezt E-vel szokták jelölni;
- Last Access Time 64 bites windows időformátumban, ezt A-val szokták jelölni.

9.4.4.3. Data Block 0x80 Resident

Az eddigi blokktípusok csak residentek lehettek, ez annyit jelent, hogy a tartalmuk mindenképpen az NTFS entryben volt tárolva. De a data block, vagyis a fájl tartalma nem biztos, hogy ide elfér. Amennyiben mégis, akkor beszélünk úgynevezett rezidensfájlokról.

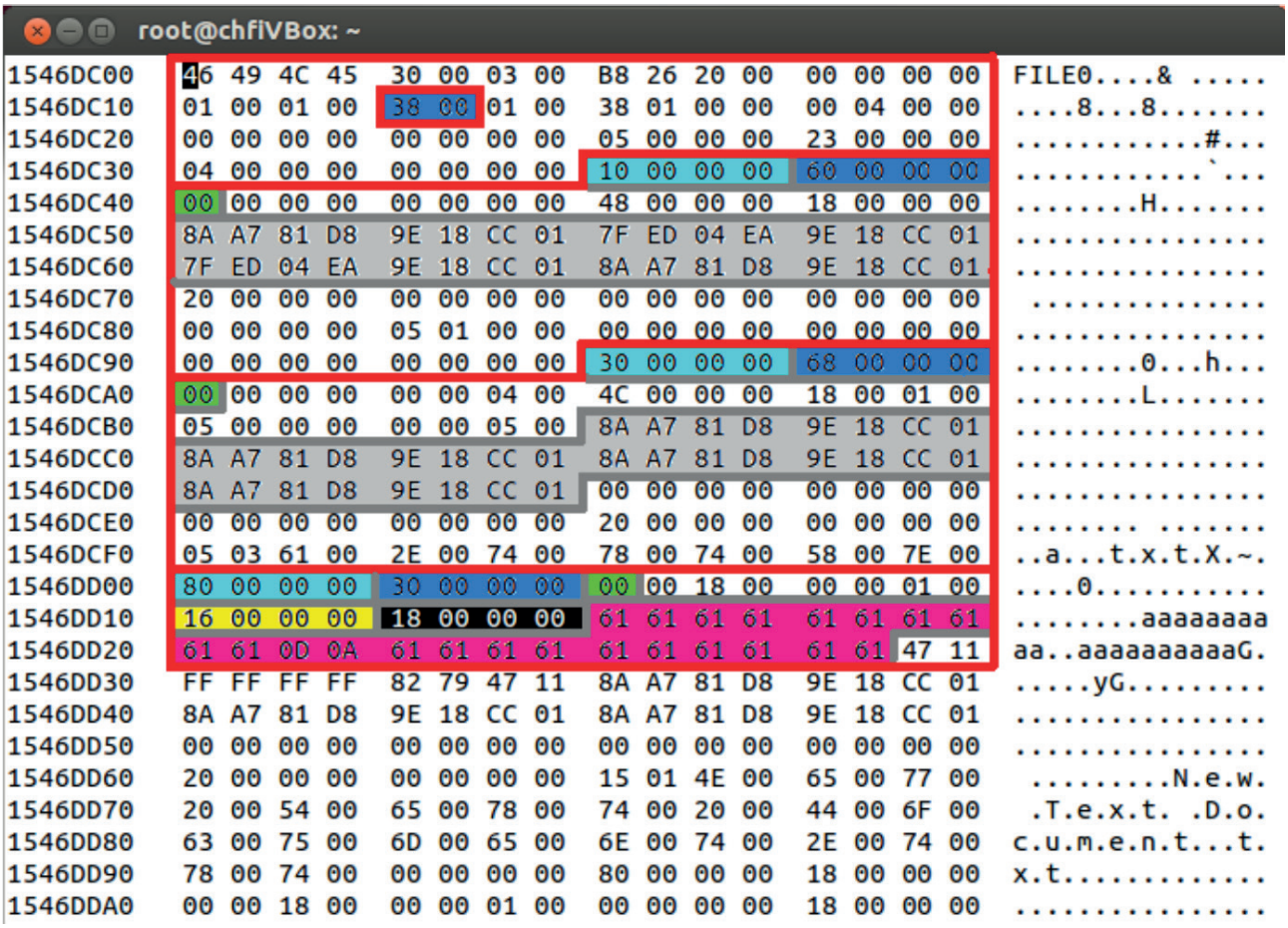


105. ábra

A Data Block 0x80 Resident felépítése

Forrás: A szerző szerkesztése

Az itt található legfontosabb információ, a fájl tartalmára vonatkozó.



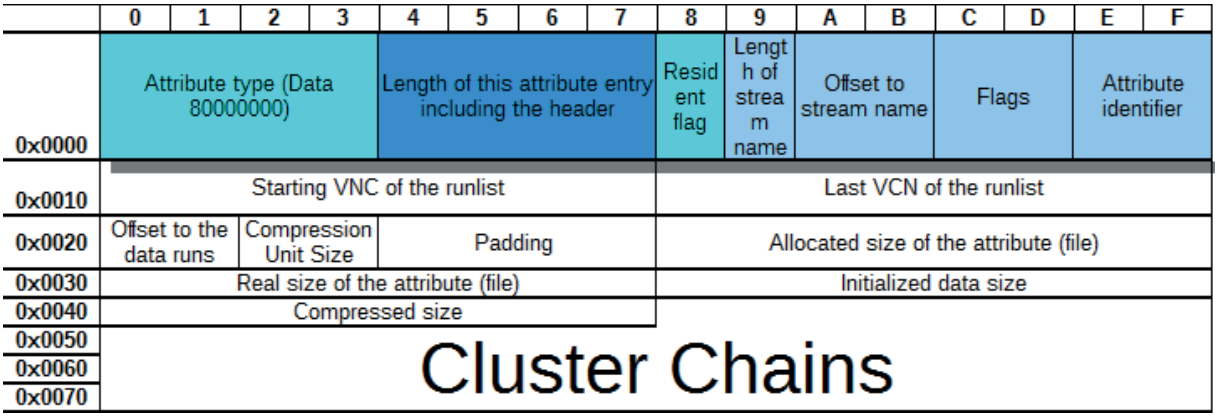
106. ábra

A fájl tartalmára vonatkozó információk

Forrás: A szerző szerkesztése

9.4.4.4. Data block 0x80 Non-Resident

Amennyiben a fájl tartalma nem fér el az NTFS entry-ben, akkor a fájltartalmat leíró clusterlista található itt.



107. ábra

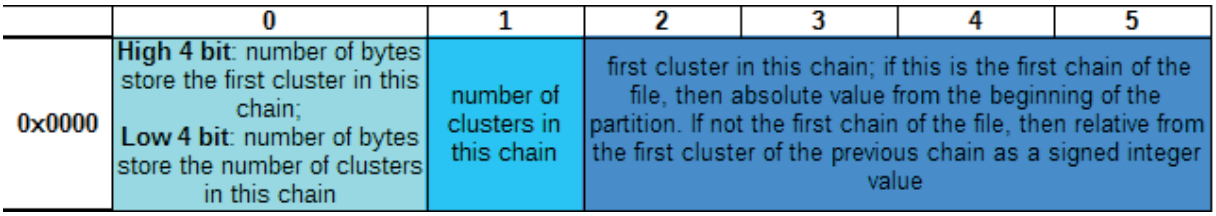
A fájltartalmat leíró clusterlista

Forrás: A szerző szerkesztése

Az itt található legfontosabb információk:

- resident flag;
- real size of the attribute;
- cluster chain.

9.4.4.5. A cluster chain felépítése



108. ábra

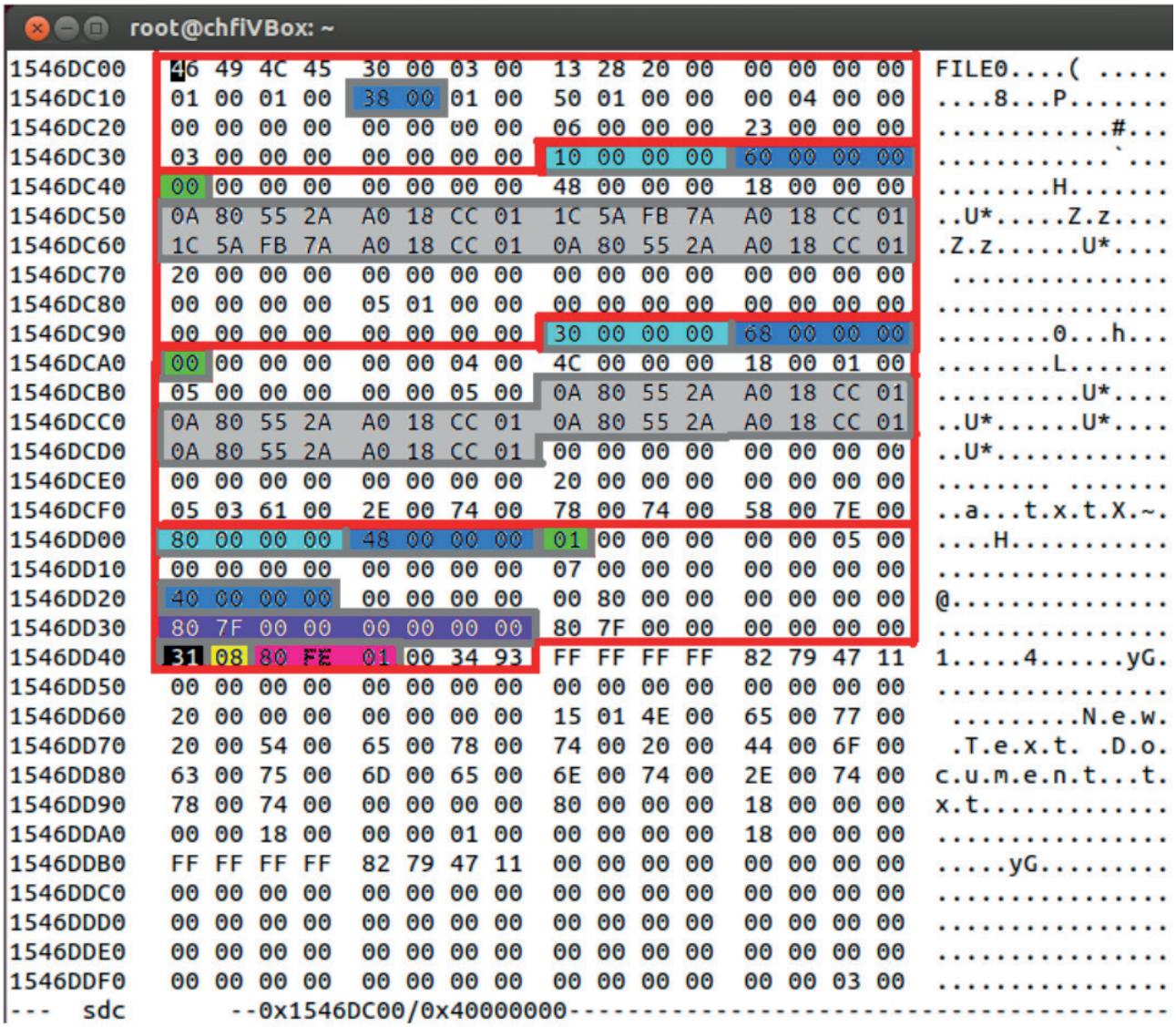
A cluster chain felépítése

Forrás: A szerző szerkesztése

A cluster chain első byte-ja két részre oszlik. A felső 4 bit adja meg, hogy hány byte-on tároljuk a cluster lánc első clusterét. Az alsó 4 bit adja meg, hogy hány byte-on tároljuk a lánc hosszát.

Amennyiben a fájl töredezett (több különálló láncból áll, nem folytonos), akkor több ilyen elem következik egymás után.

Az utolsó lánc után egy null byte zárja le a fájl cluster láncait.



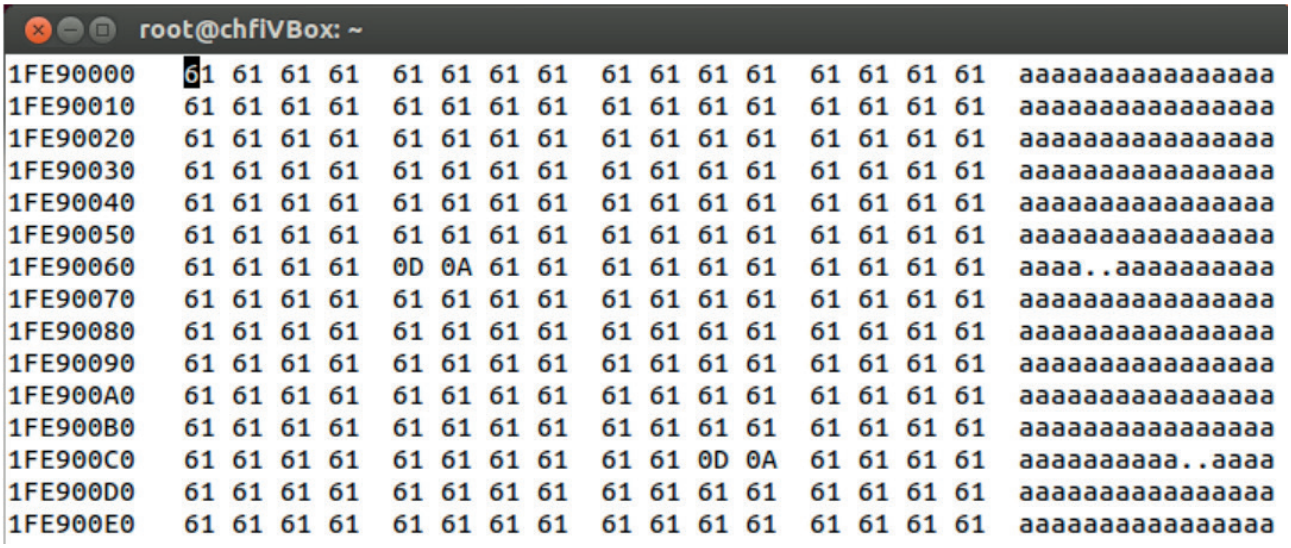
109. ábra

Egy cluster chain

Forrás: A szerző szerkesztése

Mint kiolvashatjuk, 3 byteon tároljuk a cluster chain első clusterét: 0x01FE80, 1 byteon tároljuk az egymást követő clustereket ebben a láncban: 0x08, és csak egy lánc alkotja a fájlt 0x00. A file mérete 0x7F80. A fájl tartalmát a következő byteon találjuk: 0x01FE80 * 0x1000 + 0x10000 = 0x1FE90000.

Ahol megtaláljuk a tartalmat:



110. ábra

A fájltartalom helyére vonatkozó információ

Forrás: A szerző szerkesztése

9.4.4.6. CMEA idők használata

A bizonyítási eljárás során sokszor felmerül kérdésnek, hogy egy adott fájl a meglévő gépen lett létrehozva, vagy máshol, ahonnan csak ide lett másolva? Erre biztos választ nem lehet adni, de következtetéseket lehet levonni az NTFS fájlrendszerben letárolt nyolc különböző idő egymáshoz viszonyított értéke alapján.

Figyelem, ezeknek az időknek a használata windows verziónként bizonyos mértékben eltér, én itt a Windows 2016-ot mutatom be. Mielőtt bármit kijelentenénk, ha egy eddig általunk nem vizsgált rendszerrel találkozunk, ellenőrizzük mi magunk a különböző eseteket, egy hasonló táblázatot készítsünk egy akár virtuális teszdisk elemzése segítségével.

1. táblázat

Ellenőrző táblázat

	2016							
	Standard Information Block				Filename Block			
	Create	Modify	Entry	Access	Create	Modify	Entry	Access
File created on this partition	create time	create time	create time	create time	create time	create time	create time	create time
File copied to this partition from another	**when copied**	original modified	original entry	**when copied**	**when copied**	**when copied**	**when copied**	**when copied**
File moved to this partition from another	original created	original modified	original entry	**when moved**	**when moved**	**when moved**	**when moved**	**when moved**
File copied to this directory from another directory on this partition	**when copied**	original modified	original entry	**when copied**	**when copied**	**when copied**	**when copied**	**when copied**
File moved to this directory from another directory on this partition	original created	original modified	**when moved**	original accessed	original created	original modified	original entry	original accessed
File created on this partition, then deleted	original created	original modified	original entry	original accessed	original created	original modified	original entry	original accessed
File created on this partition, then renamed	original created	original modified	**when renamed**	original accessed	original created	original modified	original entry	original accessed
File created on this partition, then modified	original created	**when modified**	**when modified**	original accessed	original created	original modified	original entry	original accessed
File created on this partition, then modified (Non-resident)	original created	**when modified**	**when modified**	original accessed	original created	original modified	original entry	original accessed
File created on this partition, then opened (resident)	original created	original modified	**when opened**	original accessed	original created	original modified	original entry	original accessed
File created on this partition, then opened (Non-resident)	original created	original modified	**when opened**	original accessed	original created	original modified	original entry	original accessed
File created on this partition, then ACL modified	original created	original modified	**when modified**	original accessed	original created	original modified	original entry	original accessed
File created on this partition, then flags modified	original created	original modified	**when modified**	original accessed	original created	original modified	original entry	original accessed

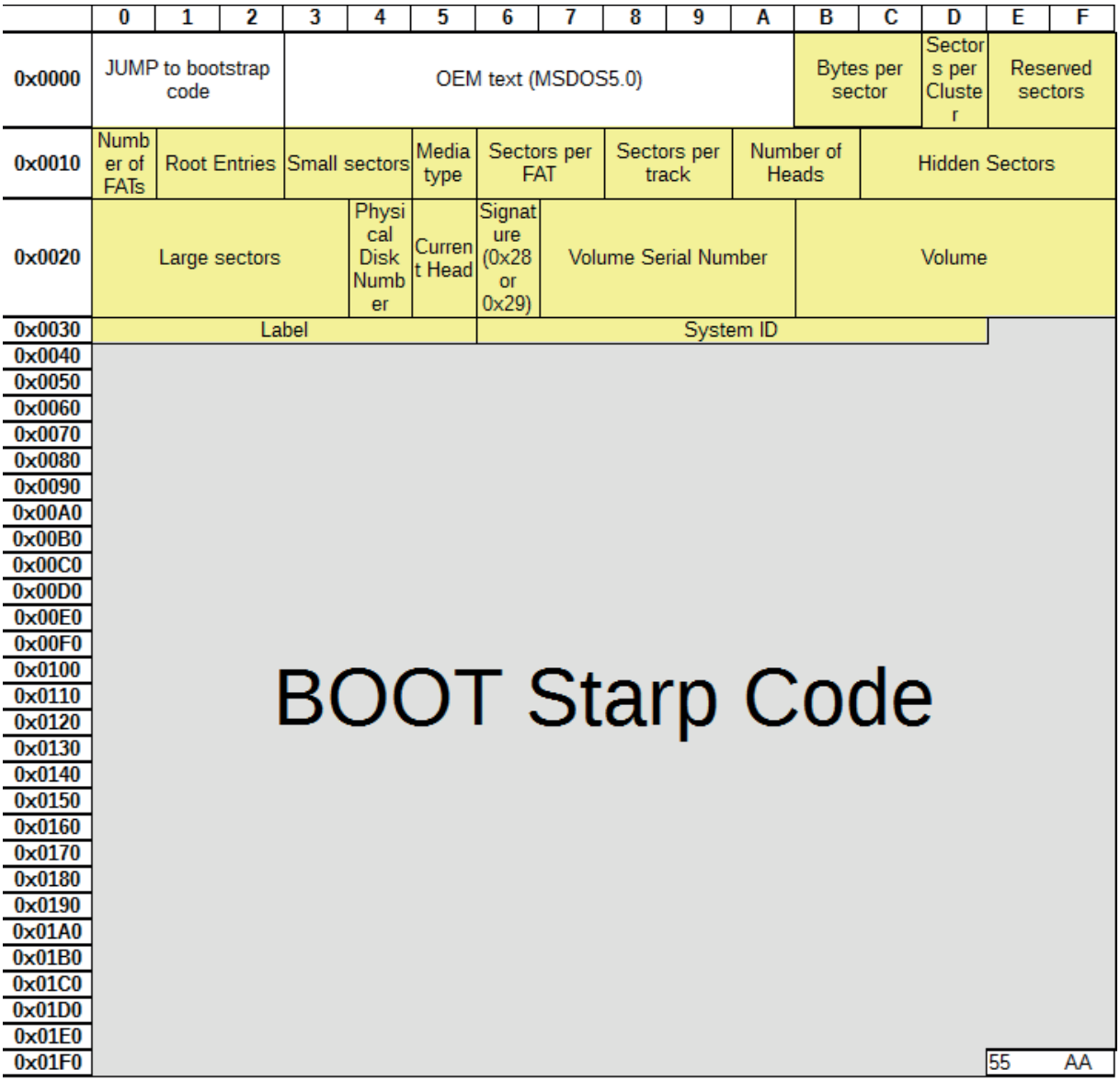
Forrás: A szerző saját szerkesztése

Érdekes módon, amikor például Notepaddal nyitunk meg egy fájlt csak olvasásra, akkor történik bejegyzés, de amikor command promptban type paranccsal kiíratjuk a fájl tartalmat, akkor nem. Tehát az egyes API hívásoktól is függhet, hogy megjelenik-e bármi is.

Szintén érdekes, hogy nem az access time változik, amikor megnyitunk egy fájlt, hanem az MFT entry time.

9.4.5. FAT fájlrendszer

FAT fájlrendszer esetében a Volume Boot Record a következőképpen néz ki:



111. ábra

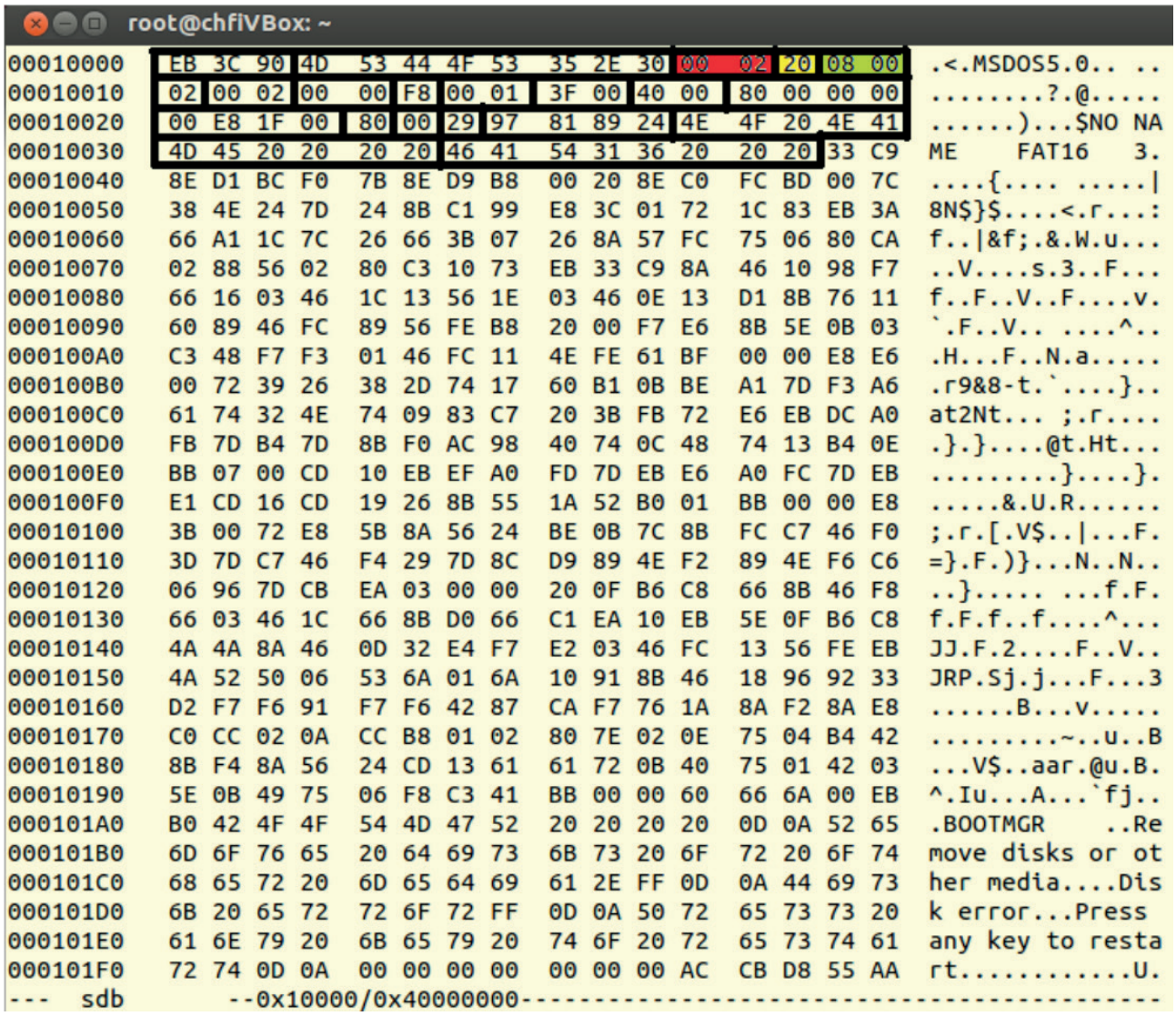
A Volume Boot Record FAT fájlrendszer esetében

Forrás: A szerző szerkesztése

Az itt található legfontosabb információk a következők:

- blokkméret, ami általában 512=0x0200;
- clusterméret, blokkokban megadva;
- a Master File Table (MFT) kezdő clustere. A Master File Table az a leíró, ami az összes többi fájlról tartalmazza a metainformációkat (például, hogy mikor hozták létre, mikor nyitották meg utoljára, mi a neve), illetve a fájltartalmat leíró clusterláncot.

Nézzünk ismét egy példát:



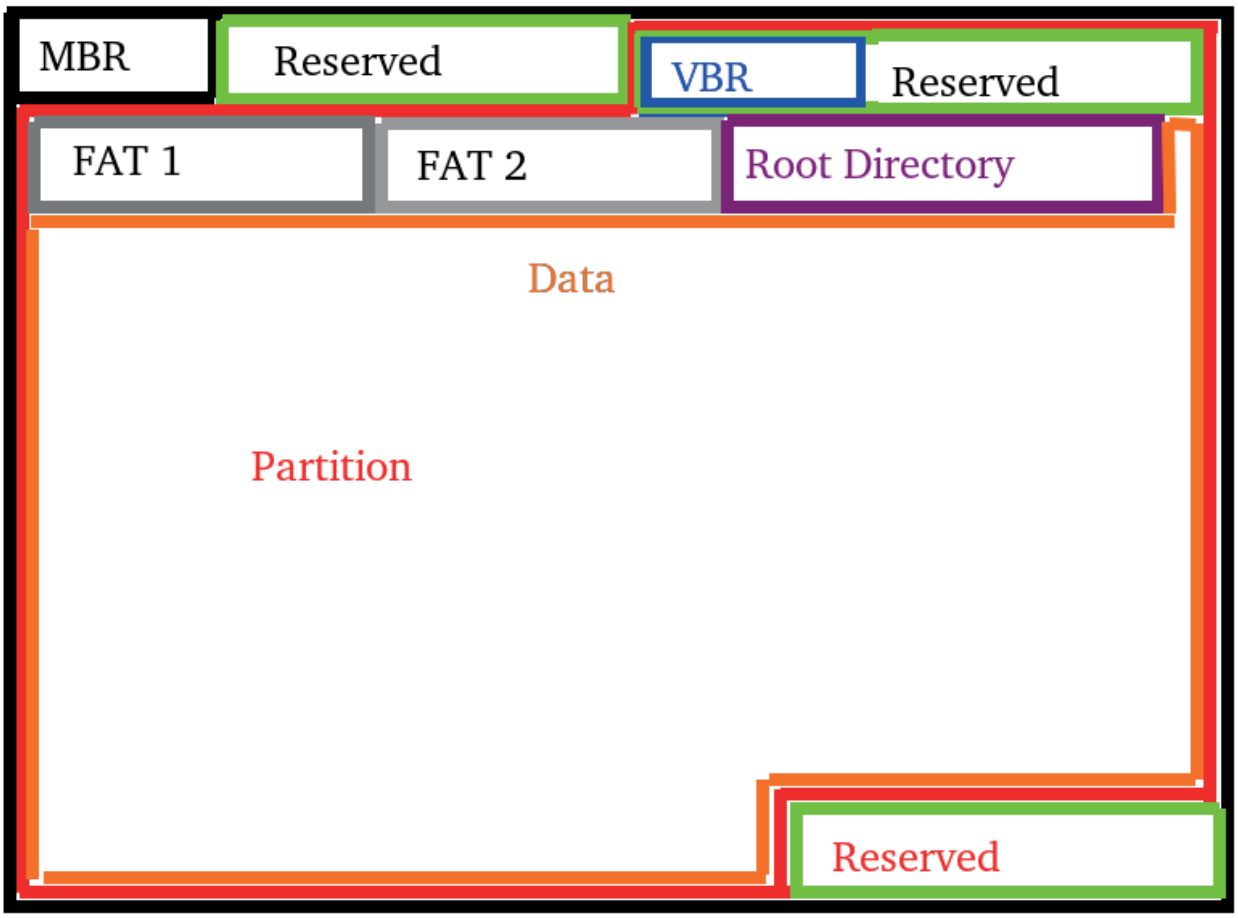
112. ábra

A FAT fájlrendszerben található információk

Forrás: A szerző szerkesztése

Itt megtaláljuk a blokkméretet (0x0200); a clusterméretet, ami 0x20 blokk, vagyis 0x0200 * 0x20 = 0x4000 = 16384 byte; a reserved szektorokat: 0x08 blokk vagyis 0x08 * 0x0200 = 0x1000 = 4096 byte; a FAT-ok számát: 0x02 (vagyis 2 FAT van). Egy FAT mérete: 0x1000 blokk, vagyis 0x0100 * 0x200 = 0x20000 byte.

Ezek alapján már kiszámolhatjuk a diskeken a fontosabb pozíciókat. Egy disk kb. a következőképpen néz ki:



113. ábra
Egy disk

Forrás: A szerző szerkesztése

Már korábbról megvan, hogy a partíció kezdete a 0x10000 pozíción kezdődik. A partíció elején a reserved block mérete: 0x1000. Vagyis az első FAT a 0x10000 + 0x1000 = 0x11000 byte-on kezdődik. A FAT mérete 0x20000 byte, vagyis a második FAT a 0x11000 + 0x20000 = 0x31000 byte-on kezdődik. A root directory kezdete: 0x31000 + 0x20000 = 0x51000 byte.

A root directoryban találhatók a fájlbejegyzések. Minden egyes bejegyzés mérete 0x20 = 32 byte, és a következőképpen néz ki (a FAT-nak rengeteg alverziója van, esetleg lehetnek minimális eltérések, például: reserved byte felhasználása, vagy kevésbé pontos időtárolás egyéb információkért cserébe).

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x0000	Filename (8+3)											Atrribu tes: 00AD VSHR	reserv ed	create time milise c	create time	
0x0010	Create date		Last access date		0x0000 if FAT16/12, high bytes of start cluster if FAT32		Last Modified Time		Last Modified Date		Start Cluster		Filesize			

114. ábra

Fájlbejegyzések a root directoryban

Forrás: A szerző szerkesztése

Lássunk erre egy példát:

root@chfIVBox: ~

```
00051000   45 56 49 44   46 41 54 31   36 20 20 08   00 00 00 00   EVIDFAT16  .....
00051010   00 00 00 00   00 00 AE 5A   D2 3E 00 00   00 00 00 00   .......Z.>......
00051020   4D 41 49 4C   32 4B 37 20   20 20 20 10   08 BA D3 5A   MAIL2K7    ....Z
00051030   D2 3E D2 3E   00 00 78 2F   B8 42 02 00   00 00 00 00   .>.>..x/.B......
00051040   4D 41 49 4C   32 4B 31 30   20 20 20 10   08 03 D4 5A   MAIL2K10   ....Z
00051050   D2 3E D2 3E   00 00 78 2F   B8 42 C3 00   00 00 00 00   .>.>..x/.B......
00051060   4D 41 49 4C   32 4B 31 33   20 20 20 10   08 29 D4 5A   MAIL2K13   ..).Z
00051070   D2 3E D2 3E   00 00 78 2F   B8 42 6B 02   00 00 00 00   .>.>..x/.Bk.....
00051080   4D 41 49 4C   39 37 20 20   20 20 20 10   08 32 D4 5A   MAIL97     ..2.Z
00051090   D2 3E D2 3E   00 00 78 2F   B8 42 CC 02   00 00 00 00   .>.>..x/.B......
000510A0   50 44 46 20   20 20 20 20   20 20 20 10   08 40 D4 5A   PDF        ..@.Z
000510B0   D2 3E D2 3E   00 00 78 2F   B8 42 30 03   00 00 00 00   .>.>..x/.B0.....
000510C0   44 4F 43 20   20 20 20 20   20 20 20 10   08 6D D4 5A   DOC        ..m.Z
000510D0   D2 3E D2 3E   00 00 78 2F   B8 42 2B 04   00 00 00 00   .>.>..x/.B+.....
000510E0   4B 45 50 45   4B 20 20 20   20 20 20 10   08 AC D4 5A   KEPEK      ....Z
000510F0   D2 3E D2 3E   00 00 96 5B   96 43 65 06   00 00 00 00   .>.>...[.Ce.....
00051100   52 4F 4F 54   46 49 4C 45   54 58 54 20   18 C0 D8 5A   ROOTFILETXT ...Z
00051110   D2 3E D2 3E   00 00 9D 4E   D2 3E 26 07   26 00 00 00   .>.>...N.>&.&...
00051120   00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00   ................
00051130   00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00   ................
00051140   00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00   ................
00051150   00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00   ................
00051160   00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00   ................
00051170   00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00   ................
00051180   00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00   ................
00051190   00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00   ................
000511A0   00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00   ................
000511B0   00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00   ................
000511C0   00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00   ................
000511D0   00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00   ................
000511E0   00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00   ................
000511F0   00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00   ................
---  sdb      --0x51000/0x40000000----------------------------------------
```

115. ábra

Fájlbejegyzés a root directoryban

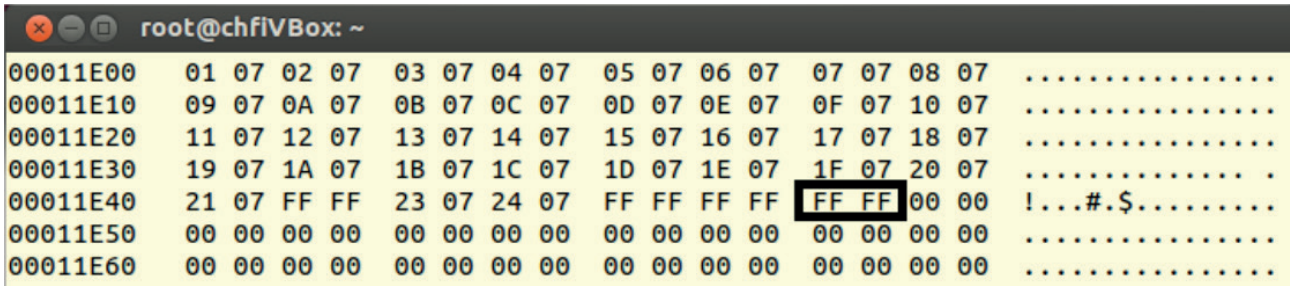
Forrás: A szerző szerkesztése

Itt a legfontosabb információk a kezdő clusterre (0x0726), illetve a fájl méretére vonatkozó (0x26 byte).

Először is megkeressük a fájlhoz tartozó bejegyzést a FAT-ban.

Tudjuk, hogy FAT16-ot használunk, vagyis egy bejegyzés 2 byteos. Így a nekünk szükséges bejegyzés a 0x0726 * 2 = 0xE4C pozíción kezdődik, a FAT elejétől számítva. Így az abszolút pozíció a FAT bejegyzéshez: 0x11000 + 0xE4C = 0x11E4C

Ott a következőt találjuk:



116. ábra

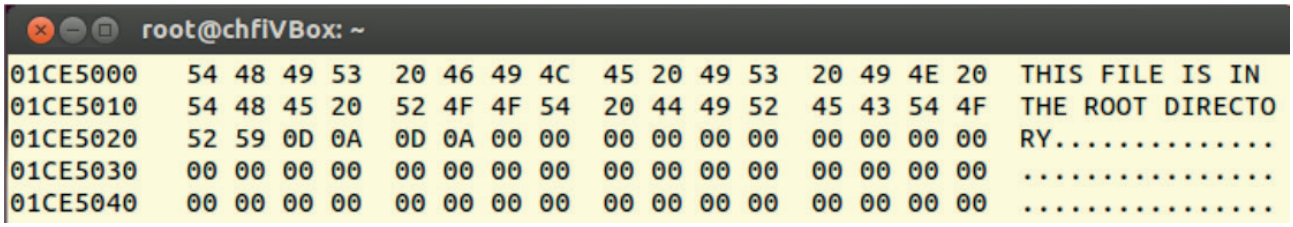
A fájlhoz tartozó FAT bejegyzés

Forrás: A szerző szerkesztése

Mivel itt 0xFFFF-et találunk, ez azt jelenti, hogy a fájl egyetlen clustert foglal el (ez a méretéből amúgy is várható volt).

A következő lépés, hogy megtaláljuk a fájl kezdetét. Ezt a következőképpen számoljuk:

(0x0726–1) * 0x20 * 0x0200 +0x051000 = 0x01CE5000



117. ábra

A fájl kezdetének megkeresése

Forrás: A szerző szerkesztése

Amennyiben a fájl nem a root directoryban van, a módszer hasonló, csak nem a root directory pozíciójában találjuk meg a fájlbejegyzéseket, hanem a disken máshol van egy ugyanilyen struktúra.

9.4.6. Software reference library-k

A vizsgálatokhoz nagy segítséget nyújt az úgynevezett software reference library. Ilyet többet is találni, talán a legnagyobb és legelterjedtebb a NIST által készített, ami letölthető a következő URL-ről: www.nsrl.nist.gov/[1] A probléma a diskek vizsgálatánál, hogy egy disken több százezer fájl lehet, ezeknek az egyesével történő átvizsgálása lehetetlen. Akkor mit lehet tenni?

A megoldás egyfelől, hogy kizárjuk a jól ismert fájlokat (például az operációs rendszer fájljai), a programcsomagok (például Office stb.) fájljait, és a maradékra koncentrálunk. Másik módszer, hogy kulcsszavakat keresünk, hiszen egy nyomozati ügynél általában meg van adva, hogy milyen jellegű információkat keresünk, azok alapján kulcsszólistát állítunk össze. Esetleg konkrét dokumentumok

[1] A letöltés ideje: 2017. április 20.

is vannak, és éppen az a cél, hogy megállapítsuk, megtalálható-e a számítógépen is, azon készült-e, ki készítette, és hasonlók. Ennek megkönnyítésére a disken található összes stringet meg lehet keresni és beindexelni (ez egyszeri, nagyon hosszú idő, akár napokba is telhet), majd utána ebben az indexelt adatban keresünk, ami már egy gyors folyamat.

9.4.7. Sleuthkit használata

Természetesen manuálisan senki nem akar minden egyes fájlt kiszedni és vizsgálgatni, inkább valami gyorsabb megoldás kell. Az egész előző leírásnak csak annyi volt a célja, hogy alapszinten megismerjük, hogyan működnek a legelterjedtebb fájlrendszerek. A leggyakoribb keretrendszer, amit használunk, a sleuthkit. Ennek az ingyenes keretrendszernek van linuxos és Windows-os változata is. Ez képes használni a legelterjedtebb imageformátumokat is, mint ewf, aff és hasonlók. Rengeteg fájlrendszert ismer, természetesen FAT, NTFS, EXT fájlrendszerek és egyebek. Gyakorlatilag, ha fájlrendszert akarunk analizálni, a sleuthkit az ingyenes de-facto standard ma.

Először is telepítsük. Ha futtatunk egy parancsot a sleuthkit-ből, és még nincsen telepítve, akkor kiírja, hogy az apt-get install sleuthkit paranccsal kell.

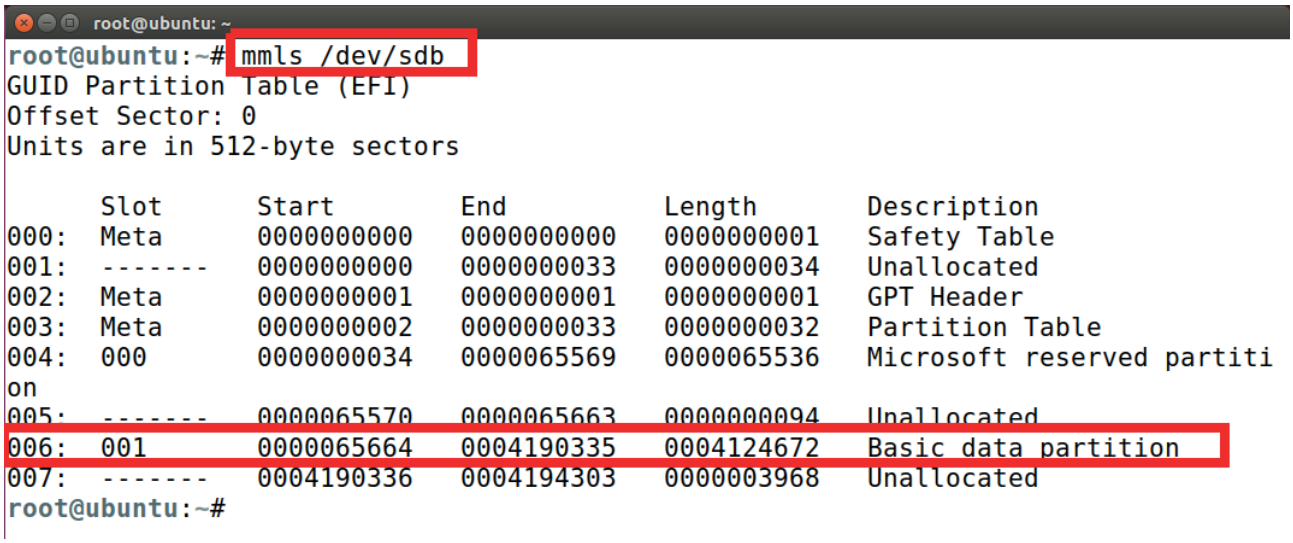
```
root@ubuntu: ~
root@ubuntu:~# mmls
The program 'mmls' is currently not installed. You can install it by typing:
apt install sleuthkit
root@ubuntu:~# apt-get install sleuthkit
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libafflib0v5 libdate-manip-perl libtsk13
Suggested packages:
  autopsy mac-robber
The following NEW packages will be installed:
  libafflib0v5 libdate-manip-perl libtsk13 sleuthkit
0 upgraded, 4 newly installed, 0 to remove and 192 not upgraded.
Need to get 1,653 kB of archives.
After this operation, 13.9 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

118. ábra

Parancs futtatása a még nem telepített sleuthkit-ből

Forrás: A szerző szerkesztése

Miután feltelepítettük a sleuthkitet, első lépésként kérdezzük le, milyen partíciók vannak. Ezt az mmls <devicenév> paranccsal tudjuk megtenni.



119. ábra

Az mmls <devicenév> parancs futtatása

Forrás: A szerző szerkesztése

A partícióinformációból megtudjuk, hogy mi a partíció offsetje: 65664.

A következő lépés, hogy listázzuk a rajta lévő fájlokat. Ehhez az fls parancsot használjuk, aminek a fontosabb kapcsolói a következők:

-l : long listet adjon, ebben benne vannak a CMEA idők is;

-p: full path-t írjon ki fájlneveknél, enlélkül + jelekkel a fájlnév előtt jelzi, hogyha az egy alkönyvtárban van;

-r: legyen rekurzív;

-o <offset>: itt adjuk meg az előbb megtudott partíció kezdet offsetet.

Az fls parancs nagyon sokáig is futhat (akát 10–20 percig), amennyiben sok fájl van a disken. Ezért nem szeretnénk sokszor futtatni, illetve a terminálból is kifut. Úgyhogy az fls kimenetét célszerű fájlba irányítani, és azzal dolgozni tovább. Ezt utána egyszerűen fel is tudjuk dolgozni, például Linuxos script fájlokkal.

120. ábra

Az fls parancs kapcsolói

Forrás: A szerző szerkesztése

A lista a következőképpen néz ki:

	A	B	C	D	E	F	G	H	I
1	metadata address	filename	Modified (Written)	Accessed (Accessed)	Entry (Changed)	Created (Created)	size	UID	GID
282	r/r 61-128-1:	enc.pst	2012-12-04 07:41:18 (CET)	2017-04-10 11:47:53 (CEST)	2017-04-10 11:23:48 (CEST)	2017-04-10 11:47:53 (CEST)	779264	0	0
283	r/r 60-128-1:	mails/mail2k13/2k13.pst	2012-12-04 07:39:48 (CET)	2017-04-10 11:47:53 (CEST)	2017-04-10 11:23:48 (CEST)	2017-04-10 11:47:53 (CEST)	779264	0	0
284	d/d 55-144-1:	mails/mail2k7	2017-04-10 11:47:53 (CEST)	2017-04-10 11:47:53 (CEST)	2017-04-10 11:47:53 (CEST)	2017-04-10 11:47:53 (CEST)	384	0	0
285	r/r 56-128-1:	mails/mail2k7/outl2007-.pst	2012-06-01 15:33:02 (CEST)	2017-04-10 11:47:53 (CEST)	2017-04-10 11:23:48 (CEST)	2017-04-10 11:47:53 (CEST)	1033216	0	0
286	r/r 57-128-1:	enc.pst	2012-06-01 15:35:36 (CEST)	2017-04-10 11:47:53 (CEST)	2017-04-10 11:23:48 (CEST)	2017-04-10 11:47:53 (CEST)	1033216	0	0
287	r/r 58-128-1:	mails/mail2k7/outlook.ost	2012-06-01 15:26:29 (CEST)	2017-04-10 11:47:53 (CEST)	2017-04-10 11:23:48 (CEST)	2017-04-10 11:47:53 (CEST)	1033216	0	0
288	d/d 66-144-1:	mails/mail97	2017-04-10 11:47:53 (CEST)	2017-04-10 11:47:53 (CEST)	2017-04-10 11:47:53 (CEST)	2017-04-10 11:47:53 (CEST)	368	0	0
289	r/r 68-128-1:	mails/mail97/outl97-.pst	2012-06-01 15:53:44 (CEST)	2017-04-10 11:47:53 (CEST)	2017-04-10 11:23:48 (CEST)	2017-04-10 11:47:53 (CEST)	525312	0	0
290	r/r 69-128-1:	mails/mail97/outl97-enc.pst	2012-06-01 15:55:33 (CEST)	2017-04-10 11:47:53 (CEST)	2017-04-10 11:23:48 (CEST)	2017-04-10 11:47:53 (CEST)	525312	0	0
291	r/r 67-128-1:	mails/mail97/outl97.pst	2012-06-01 15:56:36 (CEST)	2017-04-10 11:47:53 (CEST)	2017-04-10 11:23:48 (CEST)	2017-04-10 11:47:53 (CEST)	525312	0	0

121. ábra

Fájllista

Forrás: A szerző szerkesztése

A *metadata address* oszlopban az r/r jelenti, hogy fájl, a d/d, hogy alkönyvtár, a * pedig azt, hogy törölt a fájl az adott egység. Az utána következő szám az NTFS bejegyzés, például az 57-128-1 azt jelenti, hogy 57. bejegyzés az MFT táblában, a 128 azt, hogy ez egy 0x80 tehat data block, az 1 pedig hogy az első data block stream.

A *filename* természetesen a fájl neve.

A *Modified* az NTFS standard information blokkjából a modified idő, az Autopsy *Written*-nek hívja ezt az oszlopot, azért írtam oda azt a nevet is.

Accessed az NTFS standard information blokkjából a last access idő, az Autopsy is így hívja ezt az oszlopot.

Entry az NTFS standard information blokkjából az NTFS entry last changed idő, az Autopsy *Changed*-nek hívja ezt az oszlopot, azért írtam oda azt a nevet is.

Created az NTFS standard information blokkjából a Create idő, az Autopsy szintén *Created*-nek hívja ezt az oszlopot.

Size a fájl mérete.

UID a user ID, ez ext fájlrendszereknél van.

GID a csoport ID, ez ext fájlrendszereknel van.

A metadata address oszlopban az egyes betűk jelentése részletesen: az első betű a filename struktúrában lévő értéket mutatja, a második a metadata struktúrában lévő érték. A kettőnek, a törölt fájlok kivételével, meg kell egyeznie:

-: unknown type;
r: regular file;
d: directory;
c: character device;
b: block device;
l: symbolic link
p: named FIFO
s: shadow
h: socket
w: whiteout
v: TSK Virtual file / directory (not a real directory, created by TSK for convenience).

Ezek után ki tudjuk szedni egy fájl tartalmát, amihez a következő információkra van szükségünk: az előbb megkapott NTFS bejegyzés, az első érték, például 57 elég belőle, a fájl neve, illetve a partíció offset, amit még az mmls paranccsal kaptunk meg. A fájl tartalmának kiírására az icat parancsot kell használni. Ez alapértelmezés szerint a standard outputra írja ki a fájl tartalmát, ezért célszerű beirányítani egy fájlba.

122. ábra

A fájl tartalmának kiírására szolgáló icat parancs

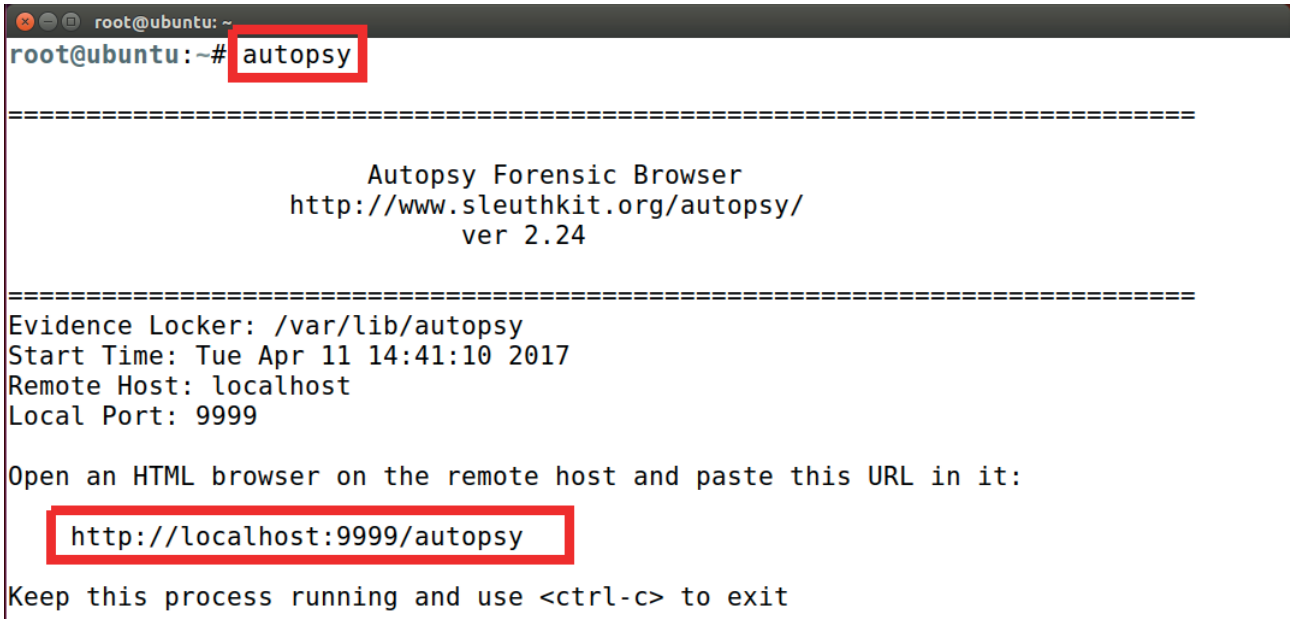
Forrás: A szerző szerkesztése

Ezek a főbb parancsok a sleuthkit-ben, de ezeken kívül még rengeteg van. Csak felsorolásszerűen: tsk_comparedir, tsk_gettimes, tsk_loaddb, tsk_recover, fsstat, ffind, ifind, ils, istat, blkcat, blkls, blkstat, blkcalc, jcat, jls, mmstat, mmcat, img_stat, img_cat, disk_sreset, disk_stat, hfind, mactime, sorter, sigfind.

9.4.8. Autopsy

A sleuthkit rengeteg parancssori eszközét nem a legkényelmesebb használni. Sok grafikus frontend létezik. Ezek közül az egyik legelterjedtebb az autopsy. Szintén létezik windowsos és linuxos verzió. A linuxos böngésző alapú, míg a windowsos egy vastagkliens. A grafikus képernyőn a gyors áttekintés sokkal kényelmesebb, de nagyobb mennyiségű adatok feldolgozására a sleuthkit scriptjei gyorsabbak tudnak lenni.

Először is indítsuk el az autopsy alkalmazást:

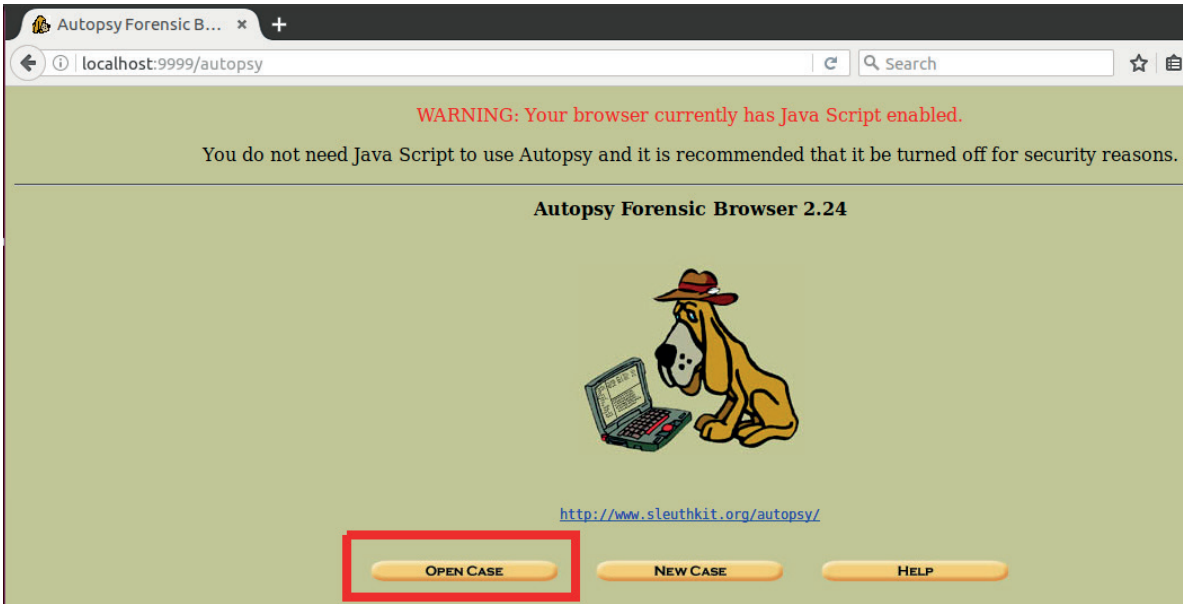


123. ábra

Az autopsy alkalmazás indítása

Forrás: A szerző szerkesztése

Miután megnyitottuk a weboldalt kattintsunk a new case vagy open case gombra.

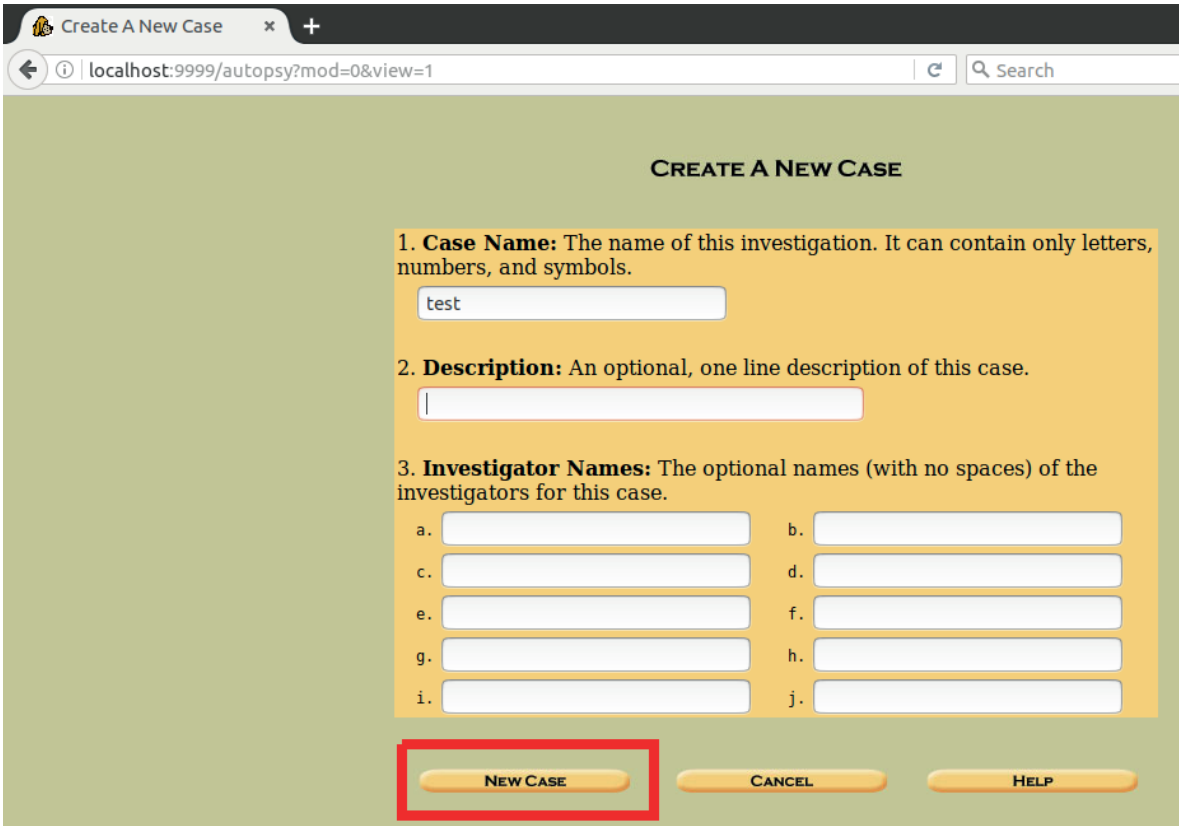


124. ábra

A weboldal megnyitását követő lépés

Forrás: A szerző szerkesztése

Adjuk meg az ügynevet, esetleg töltsük ki a többi mezőt is értelemszerűen, majd kattintsunk a New Case gombra:



125. ábra

A szükséges adatok megadása

Forrás: A szerző szerkesztése

Hozzá kell adni az egyes hostokat, ehhez kattintsunk az Add Host gombra!

126. ábra

Hostok hozzáadása I.

Forrás: A szerző szerkesztése

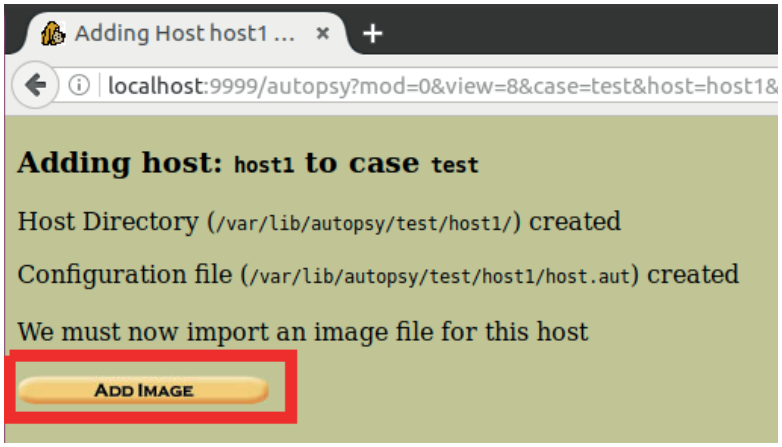
Adjuk meg a host nevét, leírást, időzónát, időeltérést, amit live analízis során feljegyeztünk. Amennyiben van, adjuk meg az ignore és az alert databaseket. Végezetül kattintsunk az Add Host gombra!

127. ábra

Hostok hozzáadása II.

Forrás: A szerző szerkesztése

Ezután meg kell adnunk az imageket, ehhez kattintsunk az Add Image gombra!

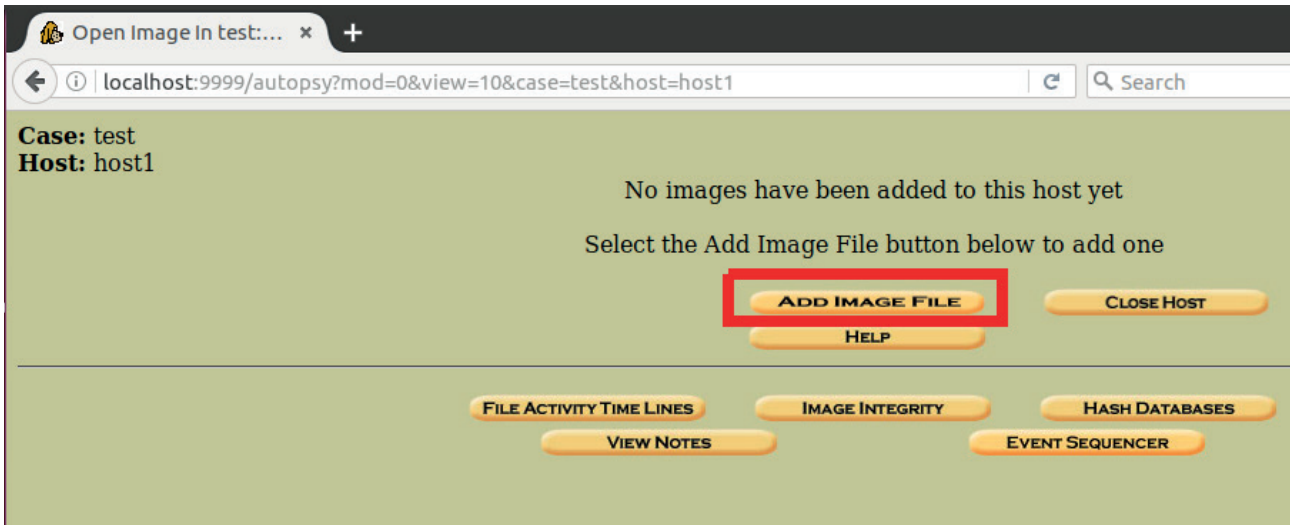


128. ábra

Imagek hozzáadása I.

Forrás: A szerző szerkesztése

A következő ablakban válasszuk az Add Image File gombot:

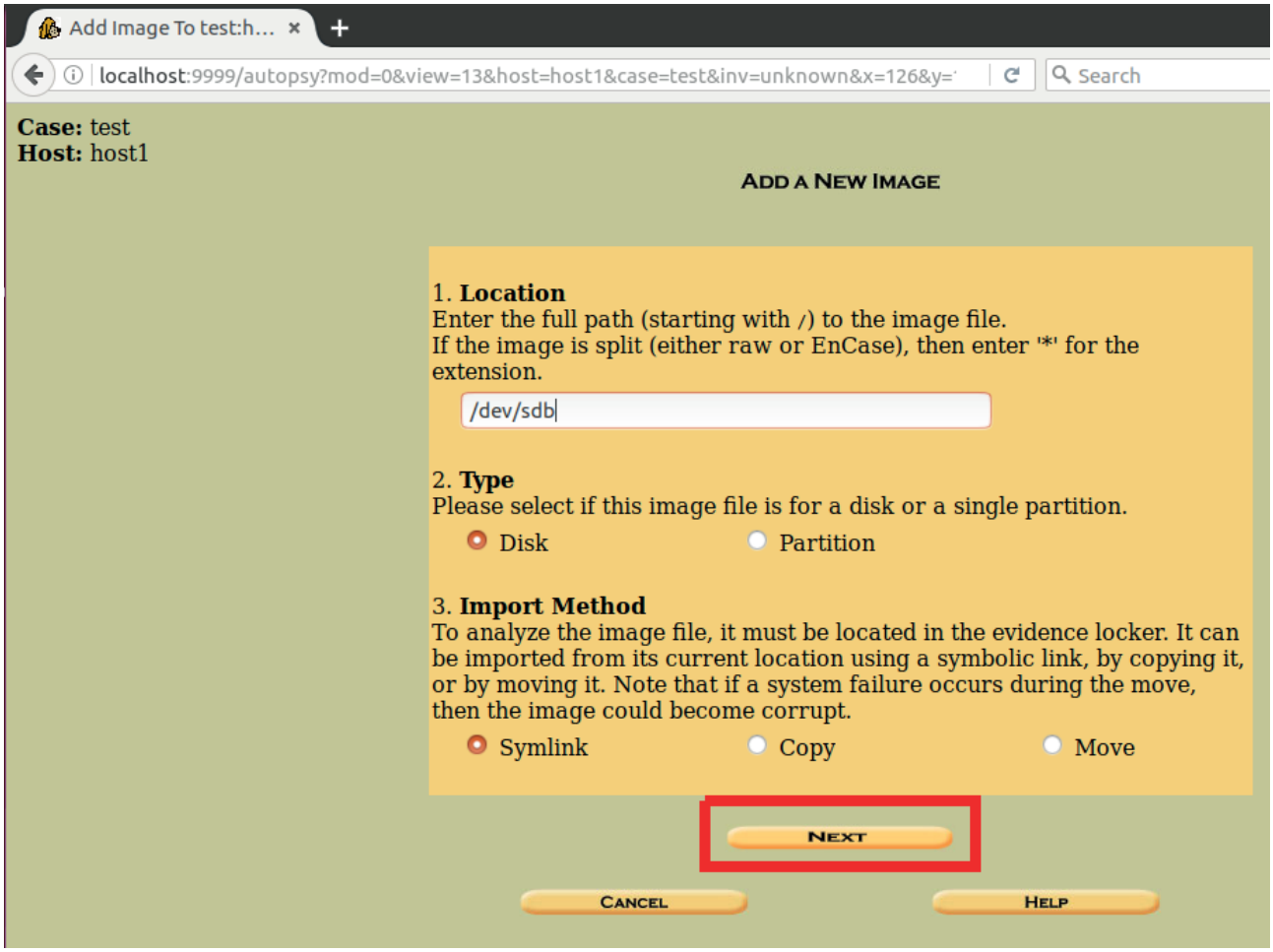


129. ábra

Imagek hozzáadása II.

Forrás: A szerző szerkesztése

Adjuk meg az image helyét. Mint látszik, az encase formátumot is ismeri. Kattintsunk a Next gombra.

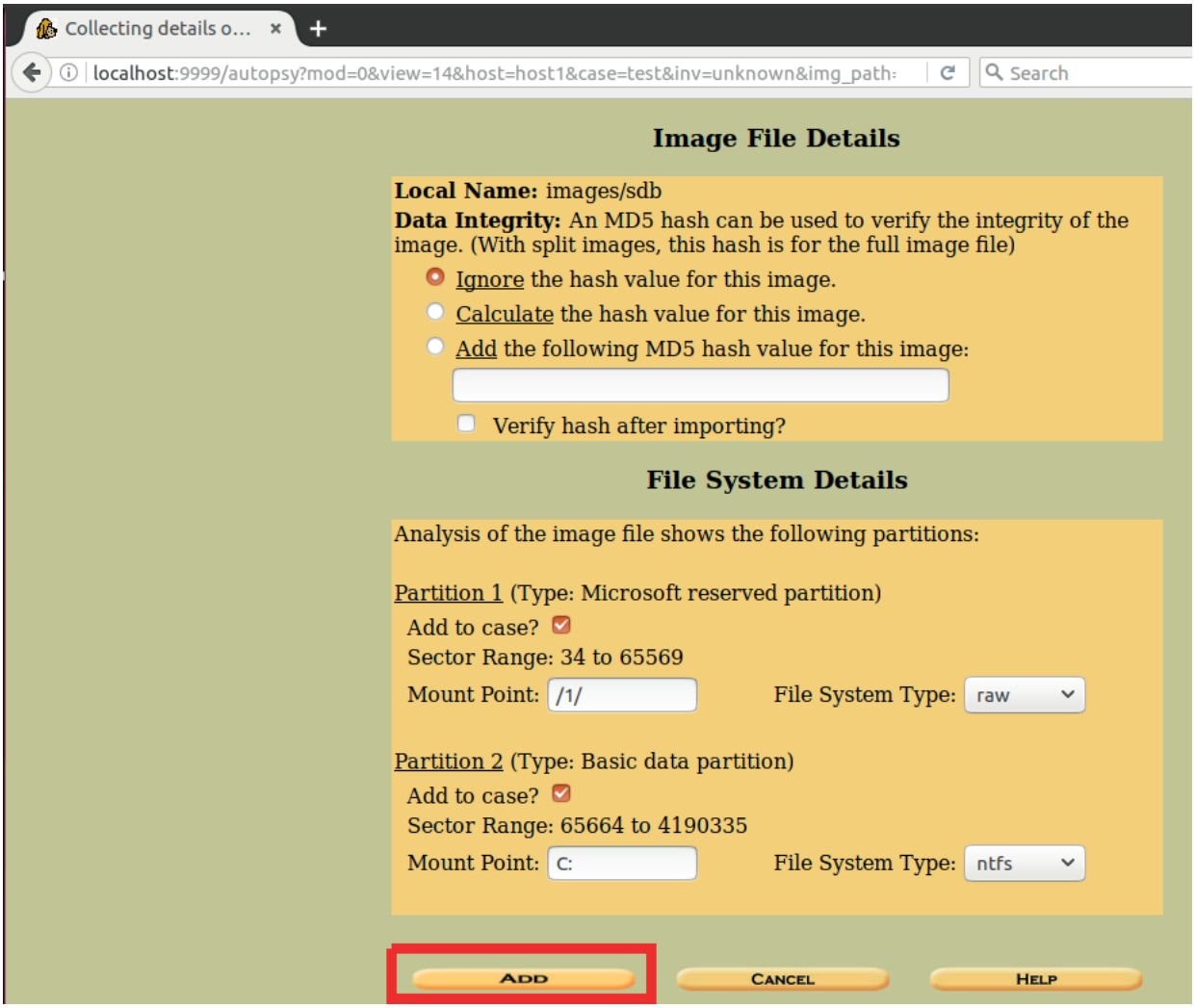


130. ábra

Image helyének megadása

Forrás: A szerző szerkesztése

Adjuk meg a disk betűjelét, majd kattintsunk az Add gombra!

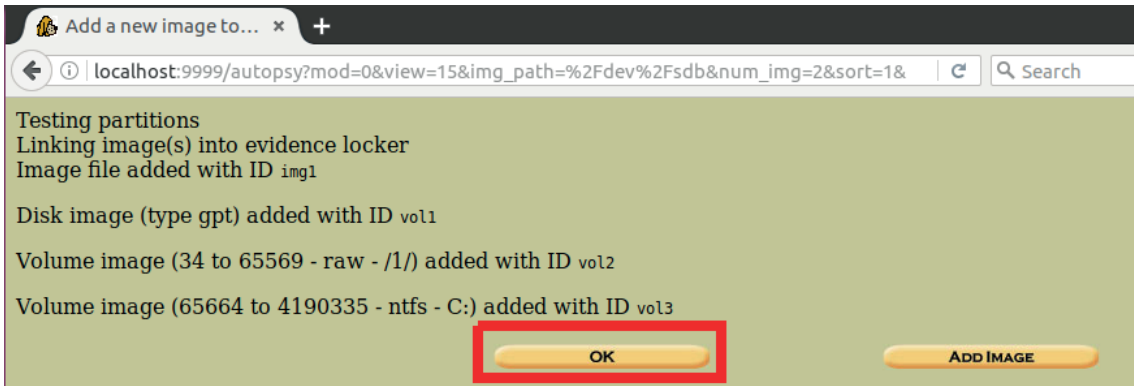


131. ábra

A disk betűjelének megadása

Forrás: A szerző szerkesztése

Nekem most nincs több imagem, úgyhogy OK.

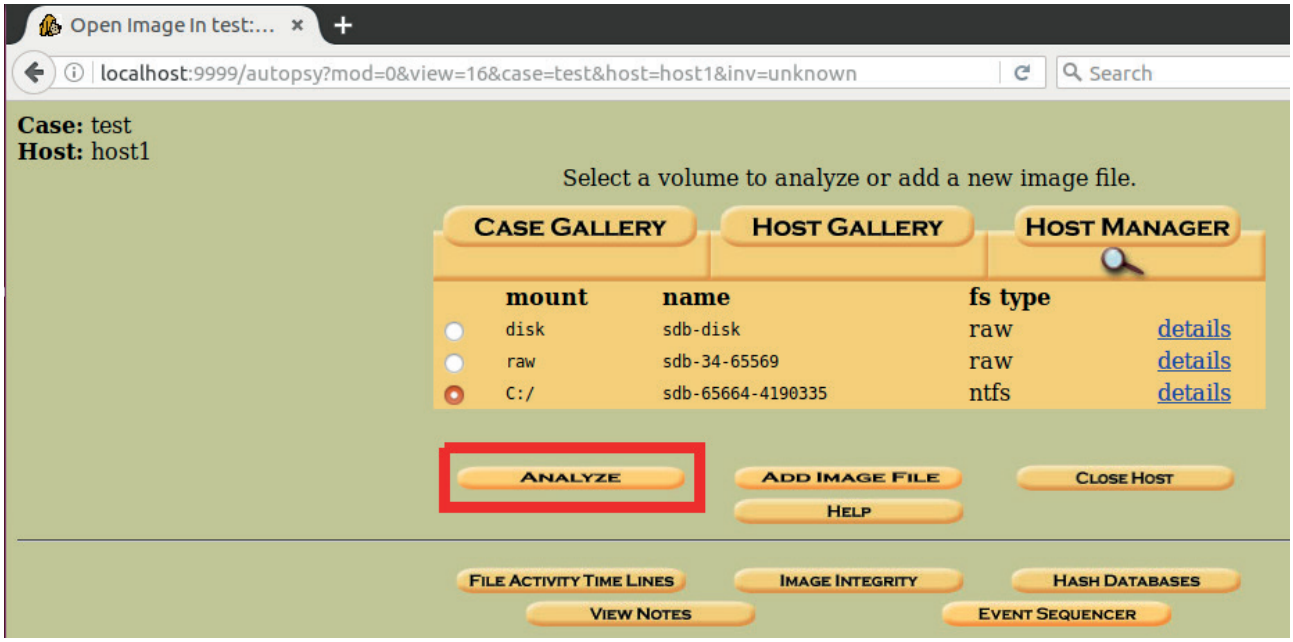


132. ábra

A diskek hozzáadásának utolsó lépése

Forrás: A szerző szerkesztése

Válasszuk ki a partíciót, majd kattintsunk az analyze gombra!

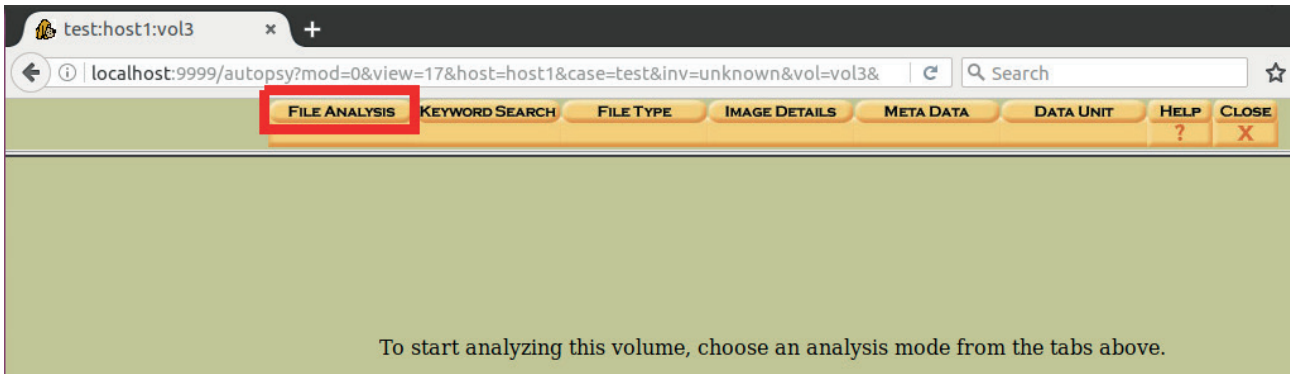


133. ábra

A partíció kiválasztása

Forrás: A szerző szerkesztése

Ezután válasszuk a File Analysis gombot!

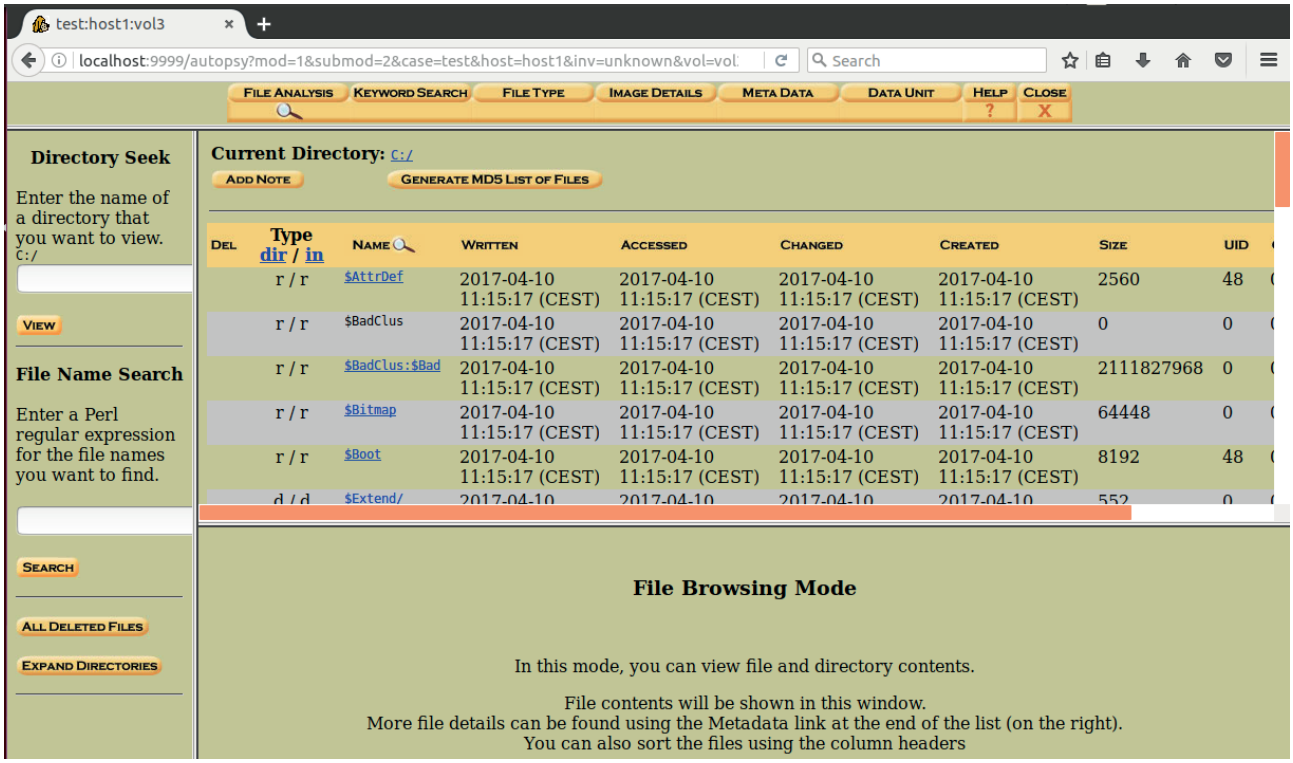


134. ábra

A File Analysis gomb kiválasztása

Forrás: A szerző szerkesztése

Itt kényelmesebben, navigálva tudjuk nézegetni a fájlokat, illetve a metaadataikat.



135. ábra

A fájlok és metaadataik

Forrás: A szerző szerkesztése

9.4.9. Törölt fájl visszaállítása

A törölt fájlok esetében két fő esetet különböztetünk meg. Amennyiben még megvan az inode bejegyzés (például MFT bejegyzés), úgy könnyű dolgunk van. Ebben az esetben a sleuthkit és autopsy, meg rengeteg egyéb alkalmazás is ugyanúgy mutatja a fájlt, mintha nem lenne törölve, ugyanúgy dolgozunk vele, mint a többivel.

Amennyiben azonban már felülíródott az inode bejegyzés (például MFT bejegyzés), nehezebb dolgunk van. Ekkor az úgy nevezet filecrawling eljárást használjuk, ami a következő képpen működik.

A fájlok általában valamilyen jól ismert headerstruktúrával kezdődnek. Ezeket keressük a disken, és amennyiben megtaláljuk, attól a pozíciótól kezdve kimásolunk egy adatmennyiséget. A kérdés, mennyit. Ez egyfelől bizonyos headerstruktúrákból kiolvasható, másfelől definiálhatunk egy bizonyos adatmennyiséget.

Mint látható, ez a módszer nagyon bizonytalan, ugyanis feltételezi, hogy a fájl folytonosan van felírva a diskre, azonban ezt semmi nem garantálja. De az operációs rendszerek azért igyekeznek a fájlokat folytonosan lehelyezni, hiszen a szekvenciális írás-olvasás kb. egy nagyságrenddel gyorsabb, mint a random. Ebből következik, hogy noha a módszer bizonytalan, azért sok esetben működni fog.

Ennek a műveletnek az elvégzésére számos alkalmazás van, például: photorec, foremost, scalpel. Ezek közül én most a foremost működését mutatom be. Amennyiben nincs telepítve, telepítsük az apt-get install foremost parancs segítségével.

```
root@ubuntu: ~
root@ubuntu:~# foremost
The program 'foremost' is currently not installed. You can install it by typing:
apt install foremost
root@ubuntu:~# apt-get install foremost
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  foremost
0 upgraded, 1 newly installed, 0 to remove and 193 not upgraded.
Need to get 38.4 kB of archives.
After this operation, 123 kB of additional disk space will be used.
Get:1 http://hu.archive.ubuntu.com/ubuntu yakkety/universe amd64 foremost amd64 1
.5.7-6 [38.4 kB]
Fetched 38.4 kB in 0s (278 kB/s)
Selecting previously unselected package foremost.
(Reading database ... 232680 files and directories currently installed.)
Preparing to unpack .../foremost_1.5.7-6_amd64.deb ...
Unpacking foremost (1.5.7-6) ...
Setting up foremost (1.5.7-6) ...
Processing triggers for man-db (2.7.5-1) ...
root@ubuntu:~#
```

136. ábra

Az alkalmazás telepítése

Forrás: A szerző szerkesztése

A foremostnak, ahogy sok más linuxos programnak, egy konfig fájlja van a /etc alkönyvtárban. Alapértelmezés szerint ennek a teljes tartalma ki van kommentezve. Ilyen esetekben a formost a beépített belső logikát használja bizonyos fájltípusok felismeréséhez. Ez jó például jpeg képekhez, amikor a fejléc nem olyan jó módszer, hiszen a jpg fejléce 0xFFD8 nagyon rövid ahhoz, hogy megbízhatóan azonosítsuk. A mélyebb struktúrák leírása azonban nehezen megoldható egy egyszerű szövegfájl használatával.

Amennyiben elkezdjük használni a config fájlt, vagyis beleteszünk legalább egy sort, a belső logika kikapcsol, és kizárólag a konfig fájlt használja.

```
root@ubuntu: ~
root@ubuntu:~# gedit /etc/foremost.conf
```

137. ábra

Fejléc

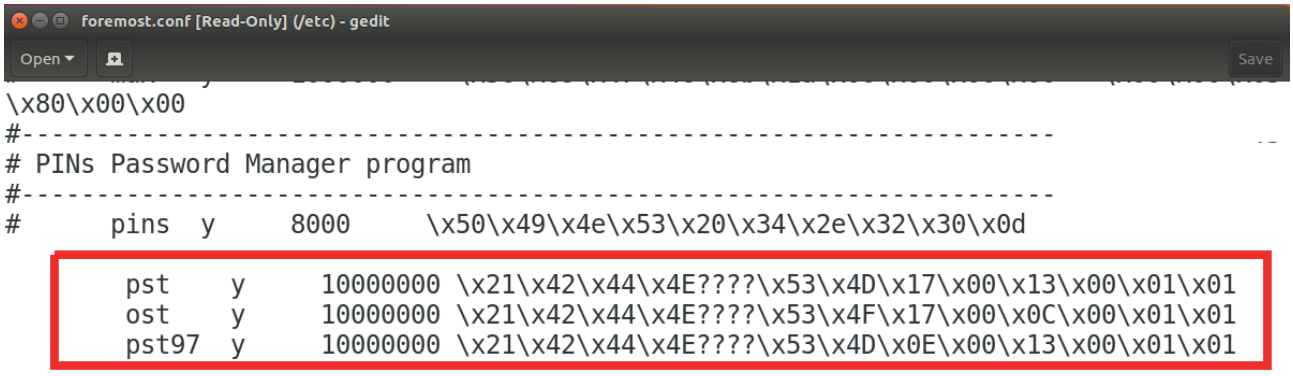
Forrás: A szerző szerkesztése

Egy sor a következő paramétereket tartalmazza:

- kiterjesztés;
- kisbetű / NAGYBETŰ érzékeny-e a minta, amit adunk y / n;
- maximális méret, amennyit kiszed, miután megtalálta a headermintát;
- headerminta;
- opcionálisan egy footer minta, hogy meddig tartson a kibontás, nem minden fájlformátumnak van footere.

Az egyes oszlopokat valamilyen whitespace szóköz vagy tabulátor választja el.

A konfigfájlban lévő alapértelmezett mintákat kezeljük fenntartásokkal, inkább sajátot használjunk.



138. ábra

Fájlinformációk a foremost-ban

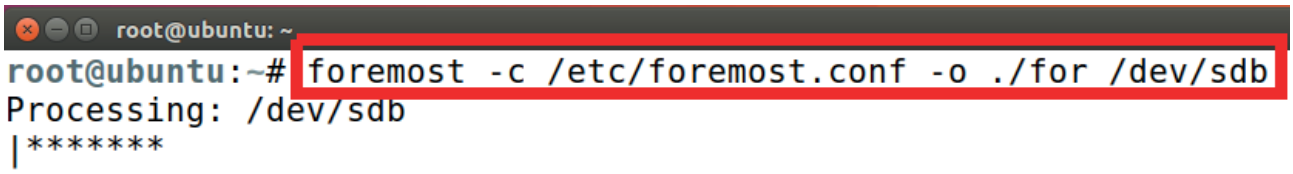
Forrás: A szerző szerkesztése

Ezek után futtassuk a foremost parancsot. Ez nem ismeri az encase és egyéb formátumokat, azokat xmount paranccsal be kell mountolni, hogy kezelni tudja őket. Én most egy egyszerű disken mutatom be.

Két legfontosabb kapcsolója:

-o output alkönyvtár neve;

-c config file, amit használunk, az alapértelmezettet nem kötelező megadni.

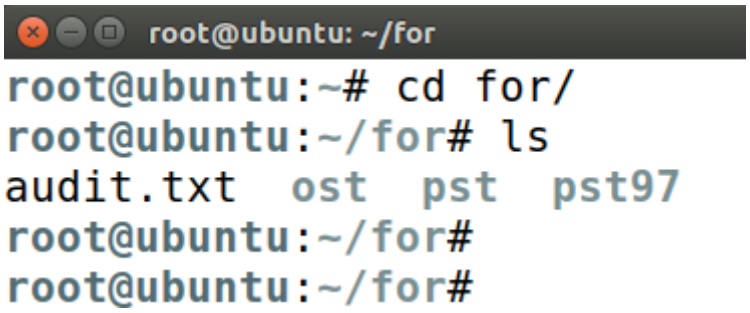


139. ábra

A foremost kapcsolói

Forrás: A szerző szerkesztése

A futás végén egy alkönyvtárszerkezetet kapunk, az általunk megadott alkönyvtáron belül minden kiterjesztésnek van egy saját alkönyvtára.

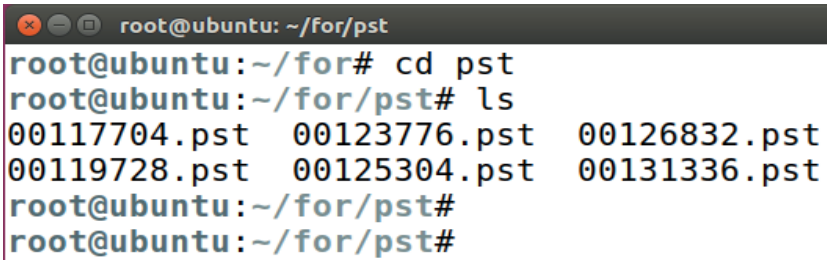


140. ábra

Alkönyvtárszerkezet

Forrás: A szerző szerkesztése

Amibe, ha belépünk, olyan típusú fájlokat találunk, ami az alkönyvtár neve.



141.ábra

A talált fájlok listája

Forrás: A szerző szerkesztése

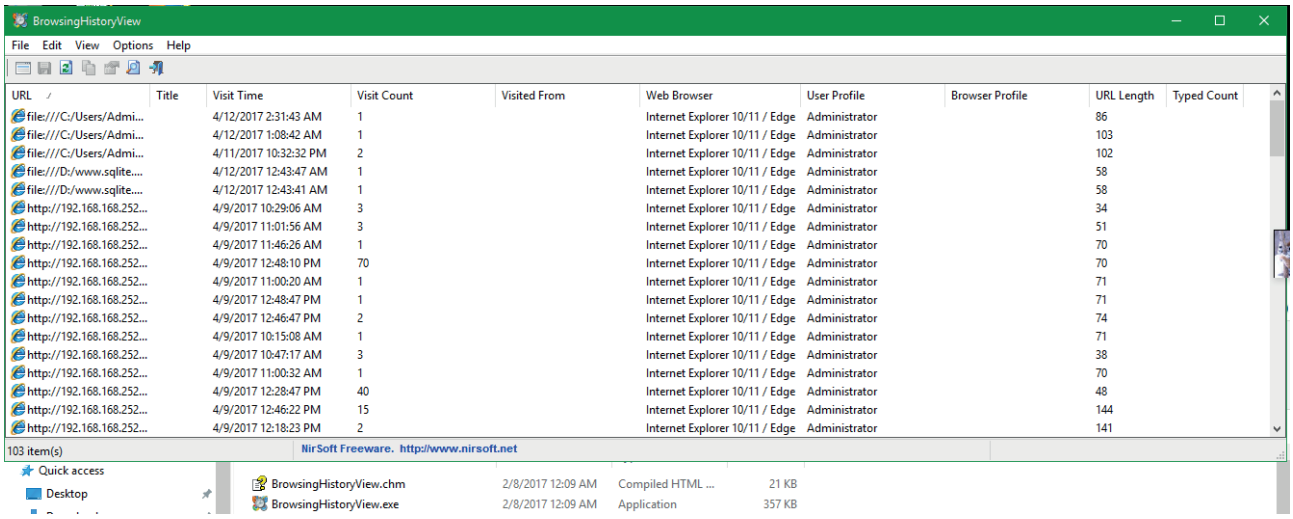
9.5. A böngészőesemények vizsgálata

A böngészők vizsgálatakor elsősorban a meglátogatott weboldalakat ismerhetjük meg. Szerencsés esetben userneveket és nagyon nagy szerencsével jelszavakat is találhatunk. Böngészővizsgálatnál az operációs rendszer nem számít, csak annyi a jelentősége, hogy hová kerülnek a szükséges fájlok. Én Windowsos böngészőkön mutatom meg.

9.5.1. Az internet explorer

Az internet explorer a historyt a fájlrendszerben tárolja, ezért nem olyan részletes, mint a később tárgyalandó chrome, illetve firefox, amik sqlite adatbázist használnak. Természetesen manuálisan is nézegethetjük a history fájlokat, de általában automata toolokat használunk, mert egyszerűbb. Böngészőanalízishez rengeteg ingyenes tool található a www.nirsoft.net weboldalon, ebben a részben ezeket fogjuk használni.

Sajnos az iehv alkalmazás csak IE10-ig működik, így az általános BrowsingHistoryView alkalmazást kell használni, ami egyszerre sok böngészőre működik. De épp ezért egyikre sem olyan részletes, mint a célzottan ahhoz készült alkalmazás.



142. ábra

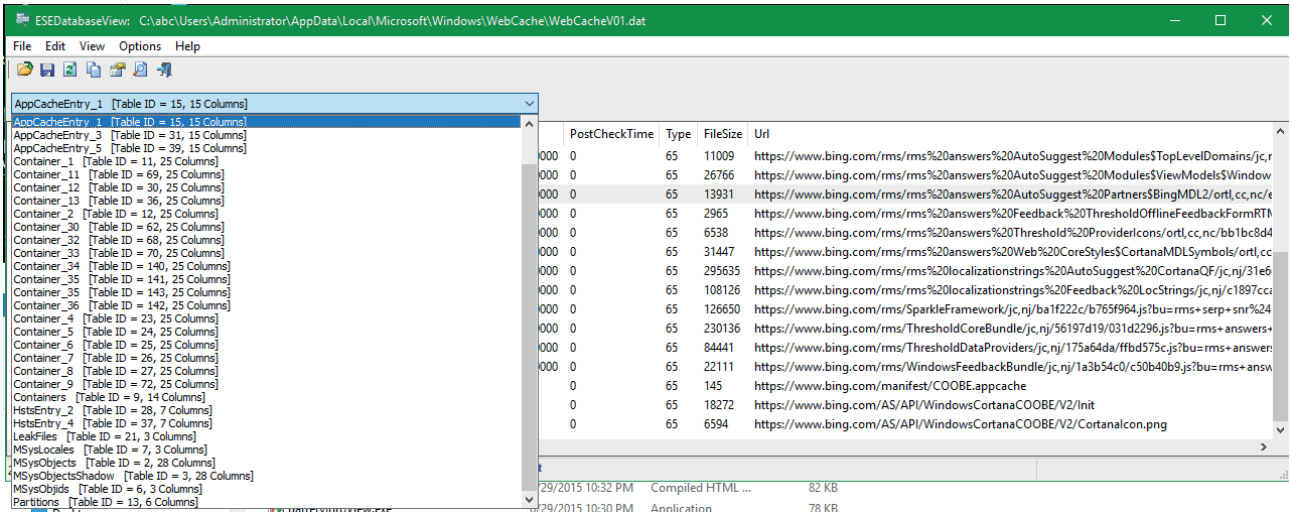
A BrowsingHistoryView alkalmazás

Forrás: A szerző szerkesztése

IE esetében a historyt az alábbi helyen találjuk:
C:\Users\Administrator\AppData\Local\Microsoft\Windows\History
(user local profil \Microsoft\Windows\History)

Edge esetében egy ESE (Enhanced Storage Engine) fájlba került. A windows előszeretettel használja ezt a formátumot, például a registry is ilyen fájl, az Active Directoryt tartalmazó ntds.dit is ilyen típusú, a search engine szintén ezt használja, de az Exchange és Microsoft SQL szerver is ennek módosított változatába dolgozik. Az adatbázis helye:
C:\Users\Administrator\AppData\Local\Microsoft\Windows\WebCache
(user local profil \Microsoft\Windows\webcache)

Az ESE fájlokat, ha valaki manuálisa szeretné megnyitni, akkor használhatja az EseDbViewer vagy ESEDatabaseView vagy esedbexport toolokat.



143. ábra

A fájlok megnyitása

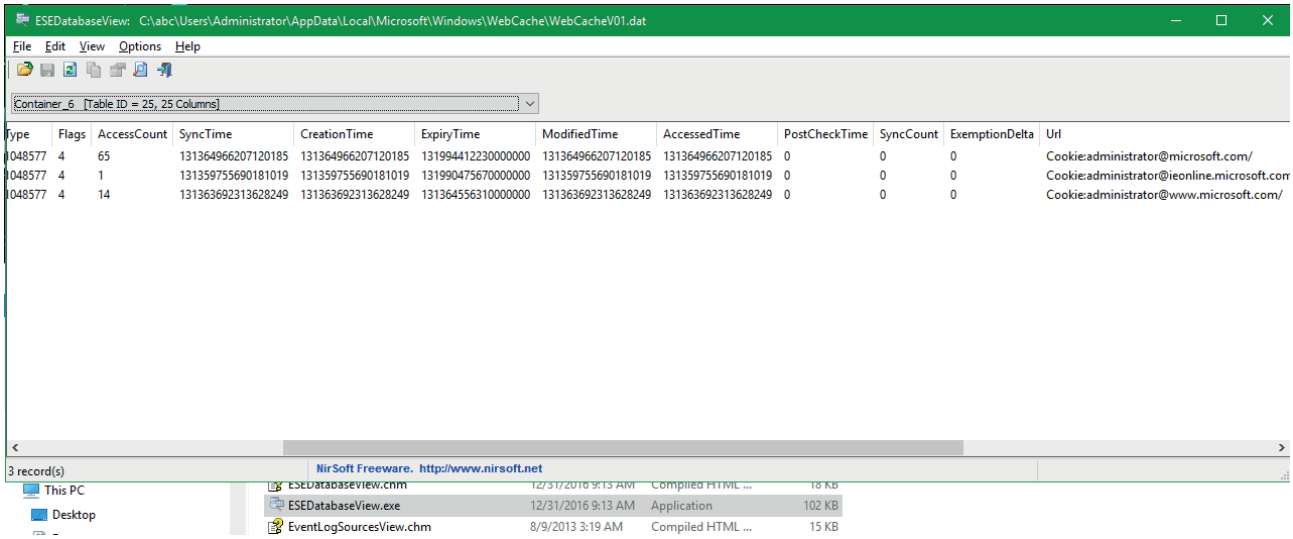
Forrás: A szerző szerkesztése

A legördülő menüben választhatunk a táblák közül.

A BrowsingHistoryView alkalmazásnak megadhatunk természetesen egy userprofilt, például egy diskimage esetében, amiből ugyanúgy kigyűjti az adatokat, mint a lokális gépből.

Másik fontos dolog, a cookie-k. Ezekben számos hasznos információt találhatunk. Legfontosabb nyilván a meglátogatott weboldalak listája. De itt találhatunk userneveket is, és ritkán, de előfordulhatnak jelszavak is.

Ezeket az iecv alkalmazással nézhetjük meg, azonban, mint előbb, ez csak IE10-ig működik. Az újabb edge az előbb említett ESE adatbázisban tárolja ezeket az információkat is.

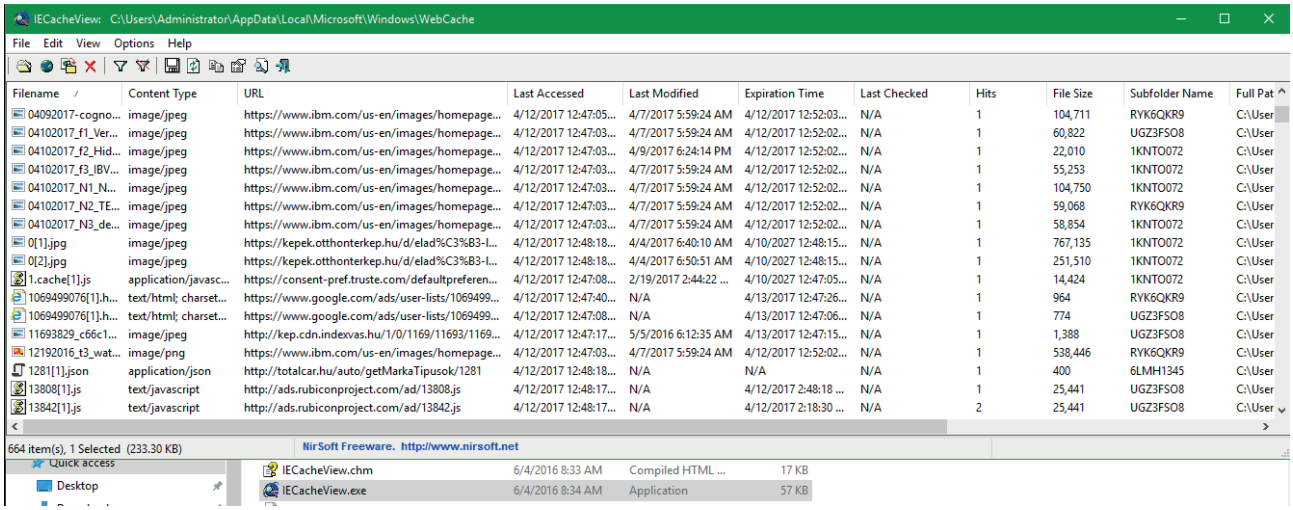


144. ábra

A cookie-k ellenőrzése

Forrás: A szerző szerkesztése

Következő hasznos információforrásunk a böngésző cache. Ehhez használjuk az IECacheView alkalmazást.



145. ábra

Az IECacheView alkalmazás

Forrás: A szerző szerkesztése

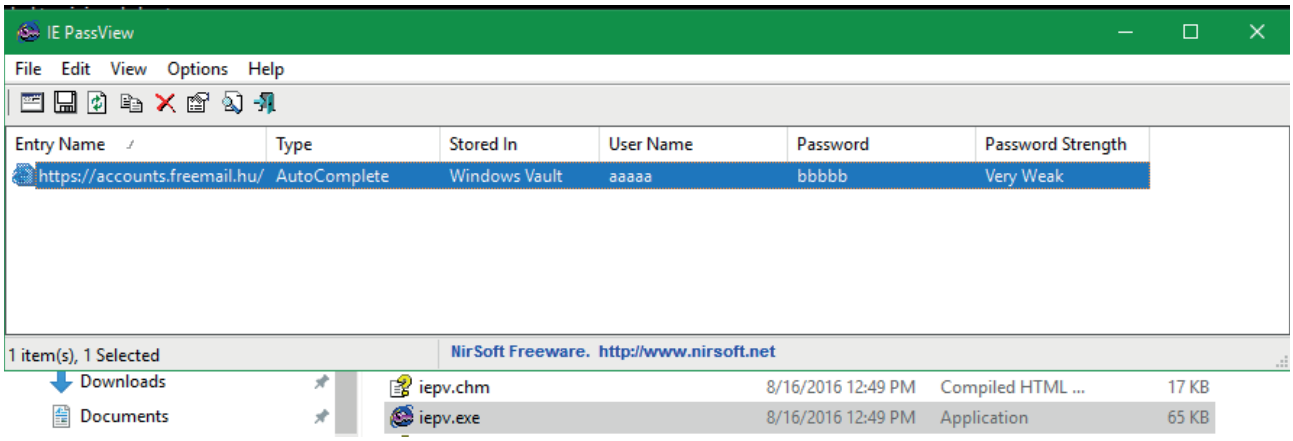
Szintén megtaláljuk a meglátogatott weboldalakat, a látogatás időpontját, továbbá a weblap részeit rekonstruálni lehet.

Ha manuálisan akarjuk megvizsgálni, akkor az adatbázis helye:
C:\Users\Administrator\AppData\Local\Microsoft\Windows\WebCache
(user local profil \Microsoft\Windows\webcache)

Végezetül megnézhetjük, hátha vannak jelszavak letárolva a böngészőkben. Ezt manuálisan nagyon nehéz visszafejteni (nyilván nem lehetetlen), ezért mindenképpen automata toolokat használjunk. A böngészők lényegében minden verzió váltáskor változtatnak jelszótárolási módot, ezért ehhez min-

denképpen frissítsük a használt alkalmazást. A jelszót a böngészőnek be kell írnia helyettünk, ezért mindenképpen visszafordítható titkosítással van letárolva. Firefoxban van lehetőség egy mesterjelszó beállítására, akkor azzal védi a letárolt jelszavakat, de a többi böngésző esetében jelen pillanatban nincs ilyen beállítási lehetőség. Ha ilyen védelemmel találkozunk, arra nem ismerünk publikus módszert, amivel tehát a mesterjelszóval levédett jelszavakat meg tudnánk szerezni a fájlokból. Amennyiben van memóriadump egy futó firefoxról, aminek meg volt adva a mesterjelszó, akkor a memóriában elképzelhető, hogy megtaláljuk a jelszavakat, de jelen pillanatban nem tudok olyan publikus alkalmazásról, amelyik ezt automatikusan megvalósítaná, vagy hogy ezt vizsgálták volna.

Az eddig használt weboldalról letölthető az iepv alkalmazás, amivel ki tudjuk iratni a jelszavakat. Ahogy a többi alkalmazásnál, parancssorból is futtatható, ahonnan az eredmény rengeteg formátumban elmenthető, így könnyen felhasználható a végső jelentéshez.



146. ábra

Az iepv alkalmazás

Forrás: A szerző szerkesztése

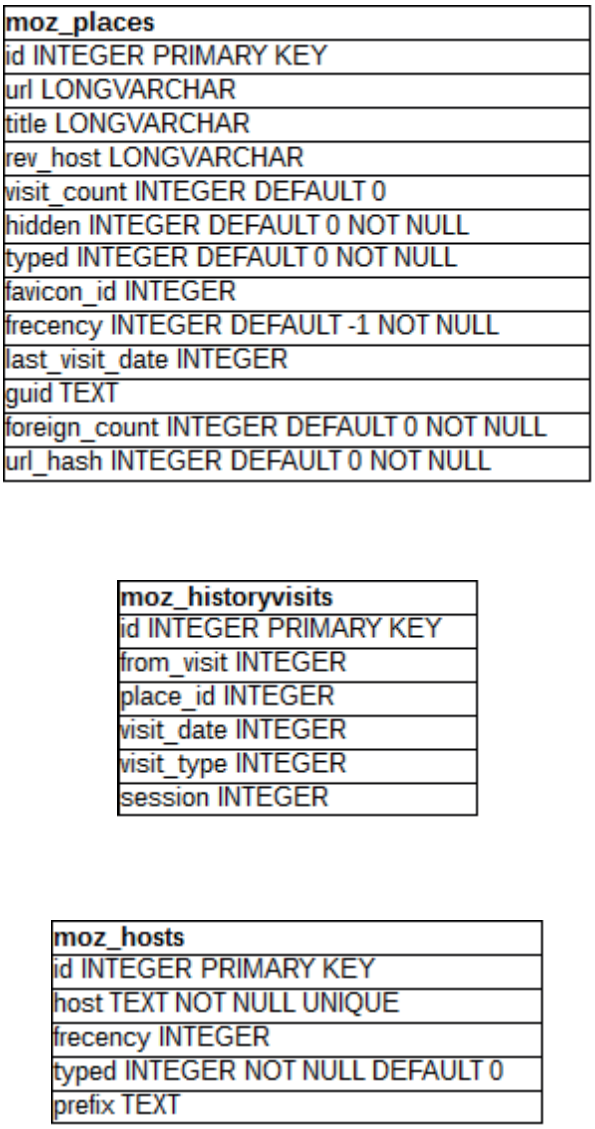
9.5.2. Firefox

A firefox a historyt SQL adatbázisban tárolja, aminek alapértelmezett helye:

C:\Users\Administrator\AppData\Roaming\Mozilla\Firefox\Profiles\<profilnév>\places.sqlite

(egyszerűbben, a roaming user profilon belül Mozilla\Firefox\Profiles\<profilnév>\places.sqlite)

Nézzük meg az adatbázis felépítésének számunkra legfontosabb részét!



147. ábra

A firefox historyt SQL adatbázisa

Forrás: A szerző saját szerkesztése

Ami nekünk leginkább kell, a moz_places tábla, amiben megtaláljuk, hogy milyen weboldalkat, és hányszor látogattak meg. Nagyon fontos mező a typed, ami 1, ha begépelték a megadott címet (vagy egy begépelt cím közvetlenül töltötte be ezt a fájlt), és 0, ha valahogy máshogy, például linkre kattintva érkeztünk ide. Fontos a visit_count, ami megadja, hogy hányszor látogatták meg a weboldalt.

Amennyiben részletesebb adatokra vagyunk kíváncsiak, akkor a moz_historyvisits táblával kell összekapcsolnunk a moz_places táblát. A moz_historyvisits place_id oszlopa kapcsolódik a moz_places id oszlopához. Ebben a historytáblában látjuk, hogy pontosan mikor látogatták meg az adott oldalt, illetve a visit_type pontosabban leírja a látogatás tipusát, ami lényeges pont lehet a szándékosságot illetően.

2. táblázat
Historytábla értelmezése

érték	név	jelentés
1	TRANSITION_LINK	Linkre kattintott
2	TRANSITION_TYPED	Begépelték, vagy elkezdték gépelni, és a felugró historyból választották ki
3	TRANSITION_BOOKMARK	Bookmarkok között kattintott rá
4	TRANSITION_EMBED	A weboldalon lévő valamilyen HTML objektum töltötte be
5	TRANSITION_REDIRECT_PERMANENT	Webszerver permanent redirect-el ide irányított
6	TRANSITION_REDIRECT_TEMPORARY	Webszerver temporary redirect-el ide irányított
7	TRANSITION_DOWNLOAD	Letöltötték

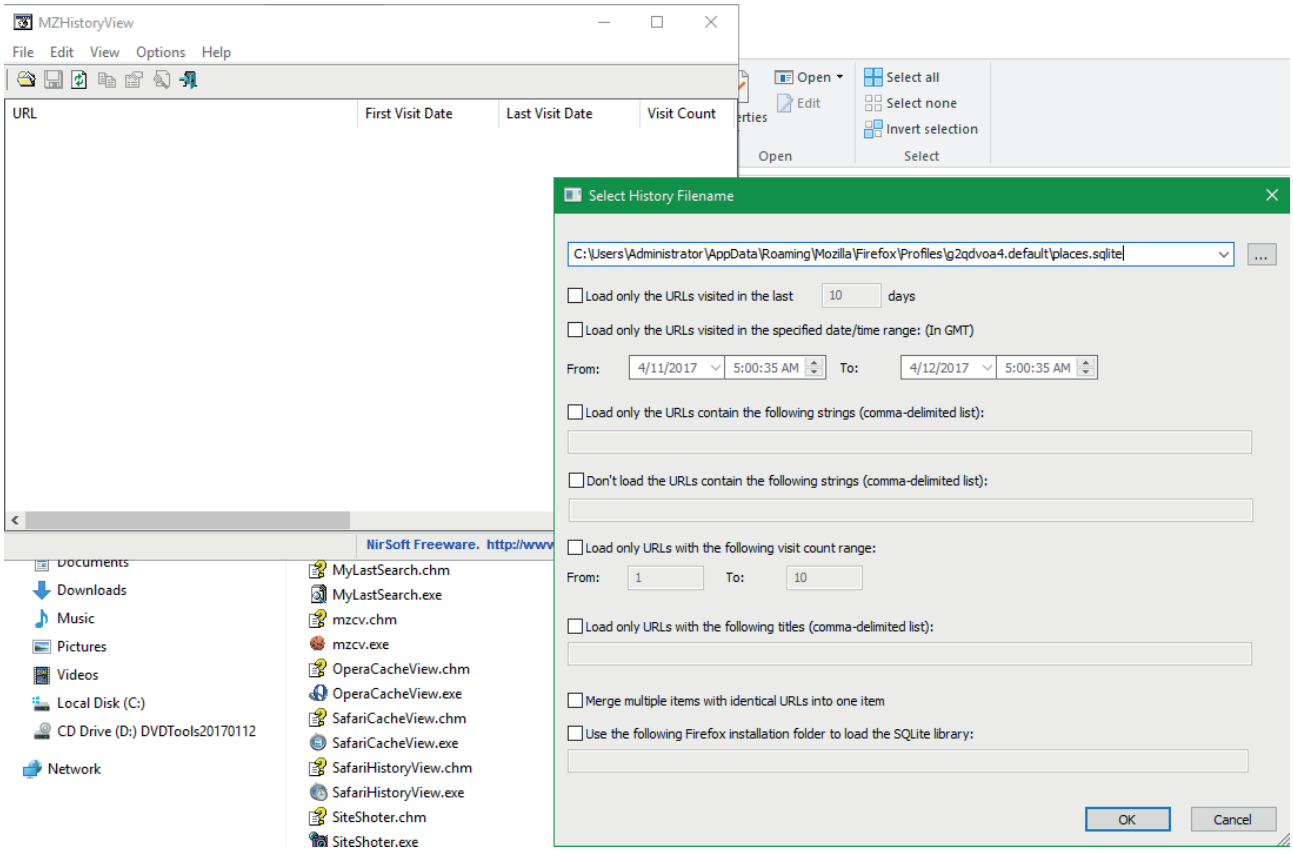
Forrás: A szerző saját szerkesztése

Amennyiben a kevésbé részletes információra vagyunk kíváncsiak, vagyis nem érdekel minket a pontos fájlnév, csak magának a meglátogatott weboldalnak a neve, akkor a moz_hosts táblát kell néznünk.

Természetesen léteznek automata toolok is ezeknek az információknak a kiszedésére, de vigyázzunk, ezek általában nem adnak meg annyi részletet, mintha közvetlenül SQL-lel kérdezzük le az adatbázist. Például sok esetben az automata toolok jelentései nem tartalmazzák a visit_type-ot, ezért fontos tudnunk, hogy manuálisan hol találjuk ezeket az információkat, és hogyan tudjuk kinyerni őket.

Az egyik legelterjedtebb browser history-t listázó eszköz a www.nirsoft.net-ről letölthető MozillaHistoryView. Ez grafikusan nagyon szépen összeszedi a látogatott weboldalakat, de parancssorból is futtathatjuk, és akkor lehetőség van az eredmény fájlba mentésére, nagyon sokféle formátumban.

Amikor elindítjuk az alkalmazást, meg kell adni a firefox sql adatbázis helyét.

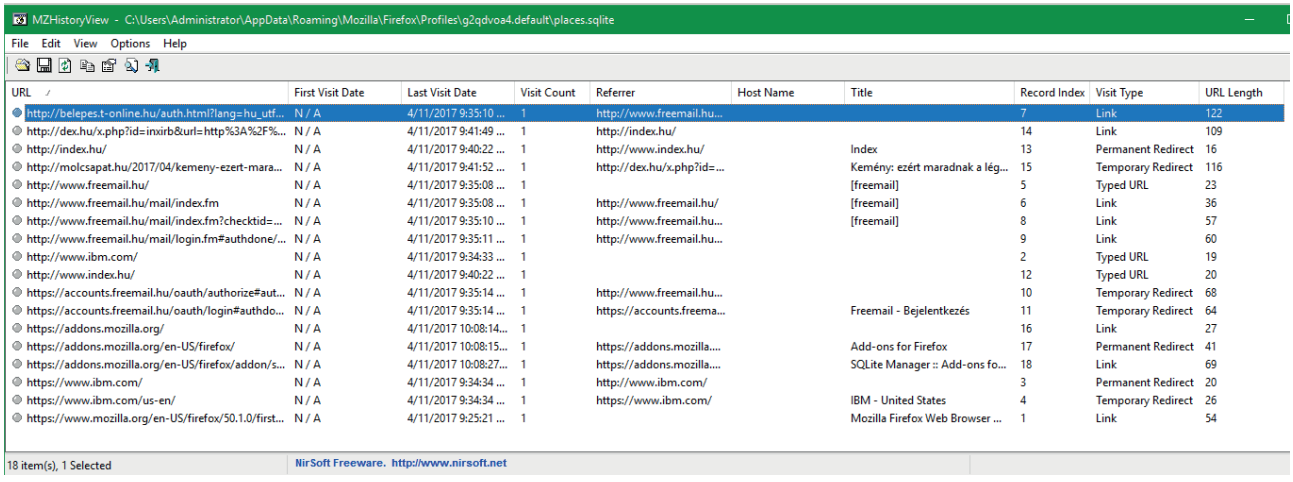


148. ábra

A MozillaHistoryView indítása

Forrás: A szerző szerkesztése

Nyilván így lehetőségünk van diskimagen lévő userprofilokból is szemezgetni. Miután megadtuk a fájlt, az alkalmazás megmutatja a history-t, a fontosabb adatokkal.



149. ábra

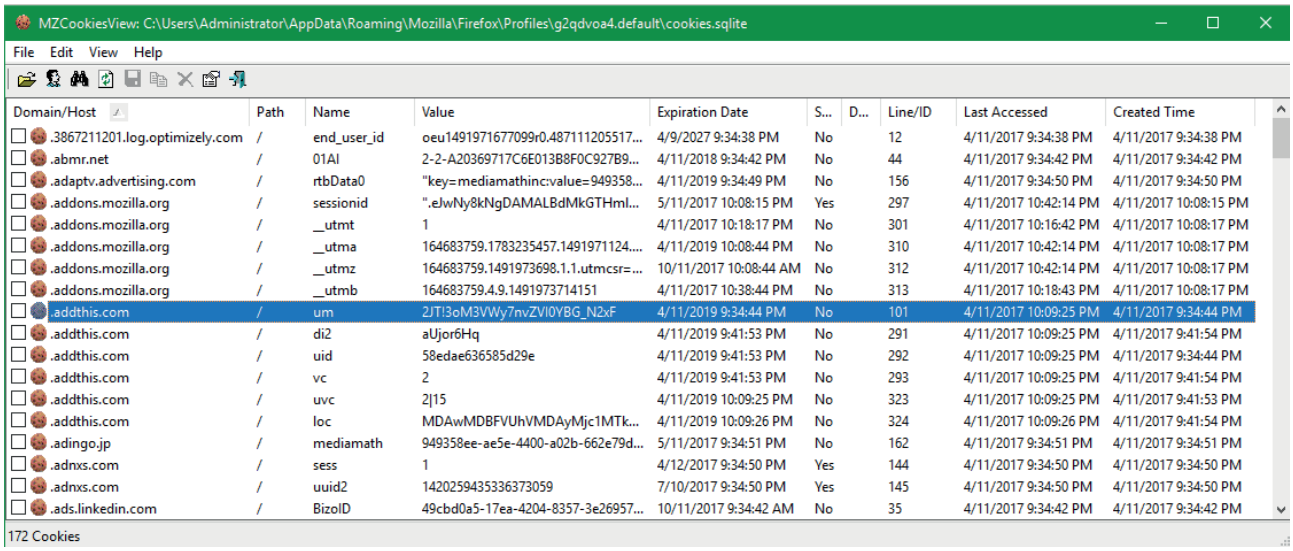
Egy fájlhoz tartozó adatok

Forrás: A szerző szerkesztése

Másik fontos dolog, amit nézhetünk, a cookie-k. Ezekben számos hasznos információt találhatunk. Legfontosabb nyilván a meglátogatott weboldalak. De találhatunk itt usernevеket is, melyek szintén

hasznosak lehetnek. Esetleg vacakabb weboldalaknál jelszó is előfordulhat, bár az azért ma már nem jellemző. Amennyiben a cookie még nem járt le, esetleg megkísérelhetünk vele belépni a felhasználó nevében a weboldalra, szintén, egyszerűbb weboldalak esetében ez sikerülhet (senki ne számítson arra, hogy majd egy gmail-ba vagy facebookba így sikerül belépni, bár egy próbát megér, de kisebb weblapoknál van rá esély.)

Ezeket szintén egyszerűbb automata eszközökkel vizsgálni már csak a cookie-k mennyisége miatt is. Az előbb említett weboldalon találjuk az mzcv nevű alkalmazást, ami hasonlóan működik az előző alkalmazáshoz, és a firefox cookie-jait mutatja meg.



150. ábra

Az mzcv alkalmazás működése

Forrás: A szerző szerkesztése

Természetesen ismét megtalálhatjuk ezeket az adatokat manuálisan is, ebben az esetben szintén egy sqlite adatbázist kell nézni. A neve:

C:\Users\Administrator\AppData\Roaming\Mozilla\Firefox\Profiles\<profilnév>\cookies.sqlite
(egyszerűbben, a roaming user profilon belül Mozilla\Firefox\Profiles\<profilnév>\cookies.sqlite)
Ebben egyetlen tábla található.

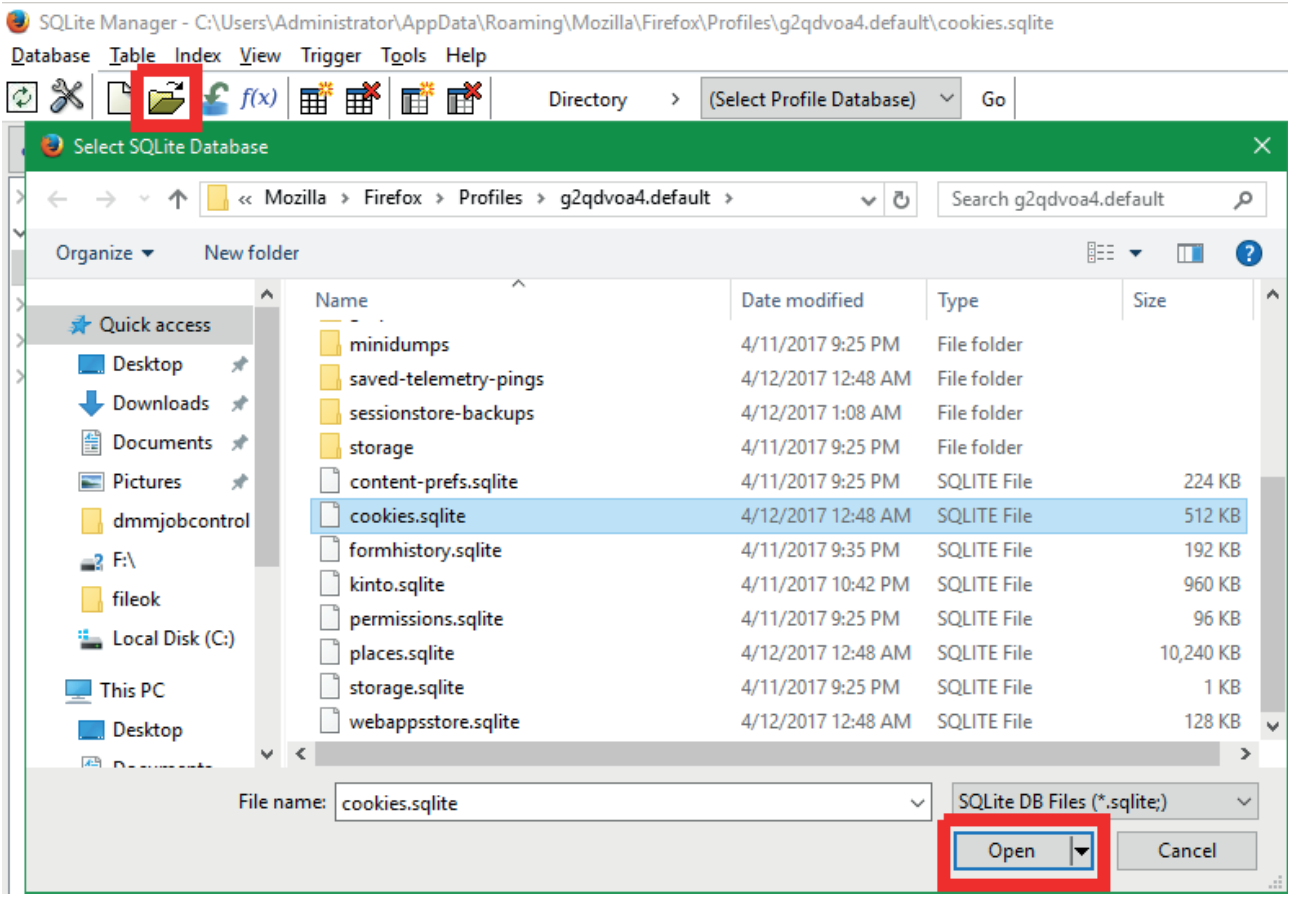
3. táblázat

A firefox sqlite adatbázisában található táblázat

moz_cookies
id INTEGER PRIMARY KEY
baseDomain TEXT
originAttributes TEXT NOT NULL DEFAULT ''
name TEXT
value TEXT
host TEXT
path TEXT
expiry INTEGER
lastAccessed INTEGER
creationTime INTEGER
isSecure INTEGER
isHttpOnly INTEGER
appId INTEGER DEFAULT 0
inBrowserElement INTEGER DEFAULT 0

Forrás: A szerző saját szerkesztése

Nyissuk meg egy sqlite adatbázis nézegetővel!

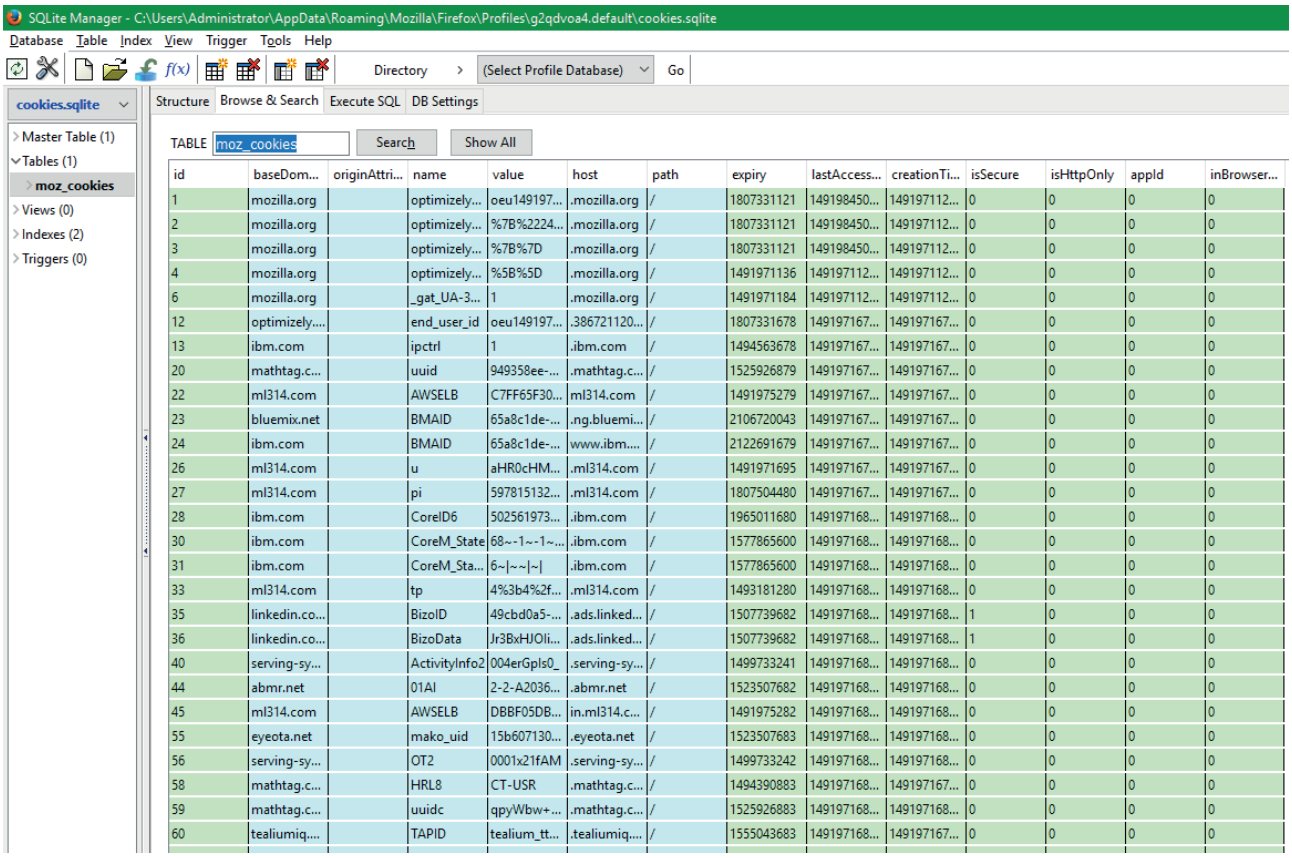


151. ábra

A firefox sqlite adatbázisának megnyitása

Forrás: A szerző szerkesztése

És vizsgáljuk meg a tartalmát!

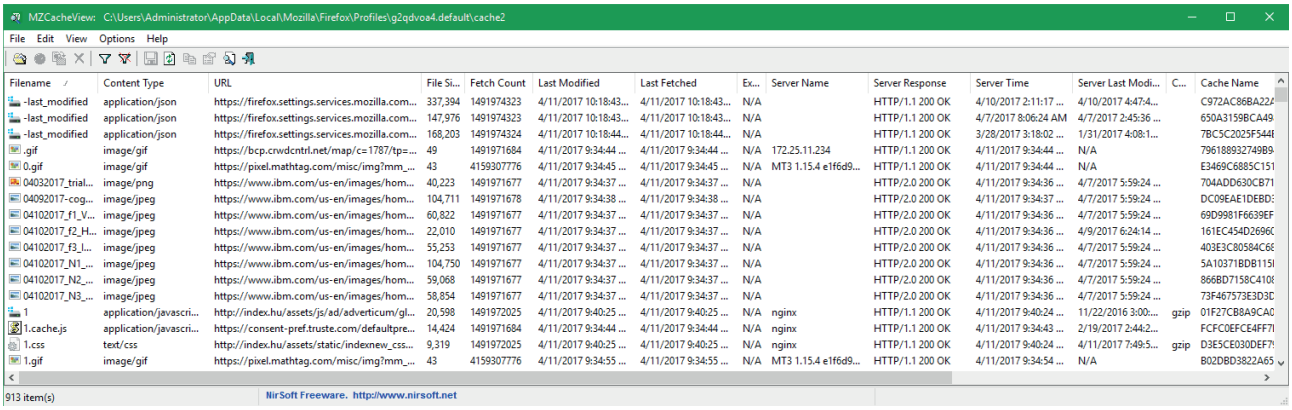


152. ábra

A firefox sqlite adatbázisa

Forrás: A szerző szerkesztése

Szintén érdemes megvizsgálni a cache tartalmát, ahol a meglátogatott weboldalakról szerezhetünk információt. Csakúgy, mint máskor, egyszerűbb, ha automata toolokkal próbálkozunk. Szintén a korábban már említett weboldalon találjuk a MozillaCacheView alkalmazást, ami megmutatja nekünk a cache tartalmát. Mint a többi alkalmazásnál, parancssorból is futtatható, ahonnan az eredmény rengeteg formátumban elmenthető, így könnyen felhasználható a végső jelentéshez.



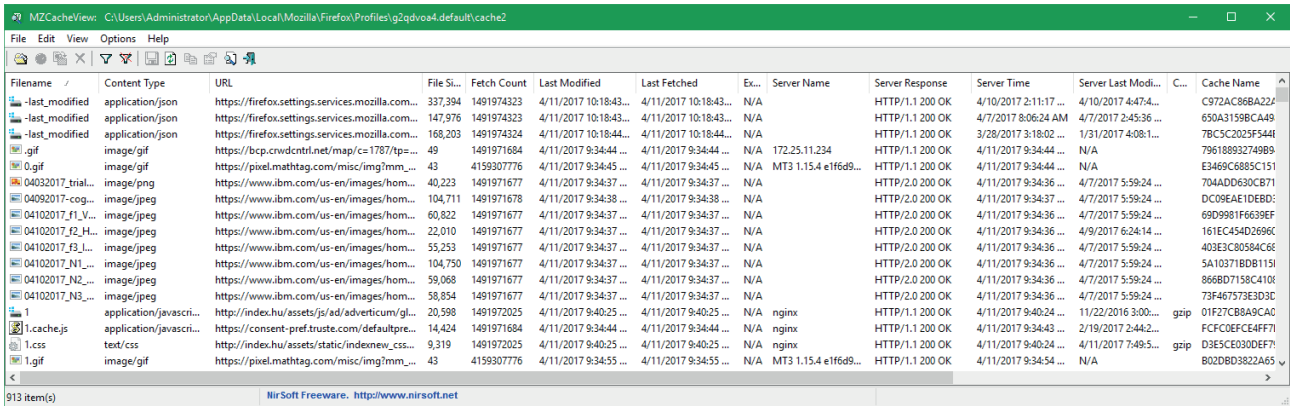
153. ábra

A MozillaCacheView alkalmazás

Forrás: A szerző szerkesztése

A cache tartalmat, ha manuálisan szeretnénk nézegetni, a következő helyen találjuk:
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\<profilnév>\cache2\entries

(egyszerűbben, a local user profilon belül Mozilla\Firefox\Profiles\<profilnév>\cache2\entries alkönyvtár)



154. ábra

A cache tartalom

Forrás: A szerző szerkesztése

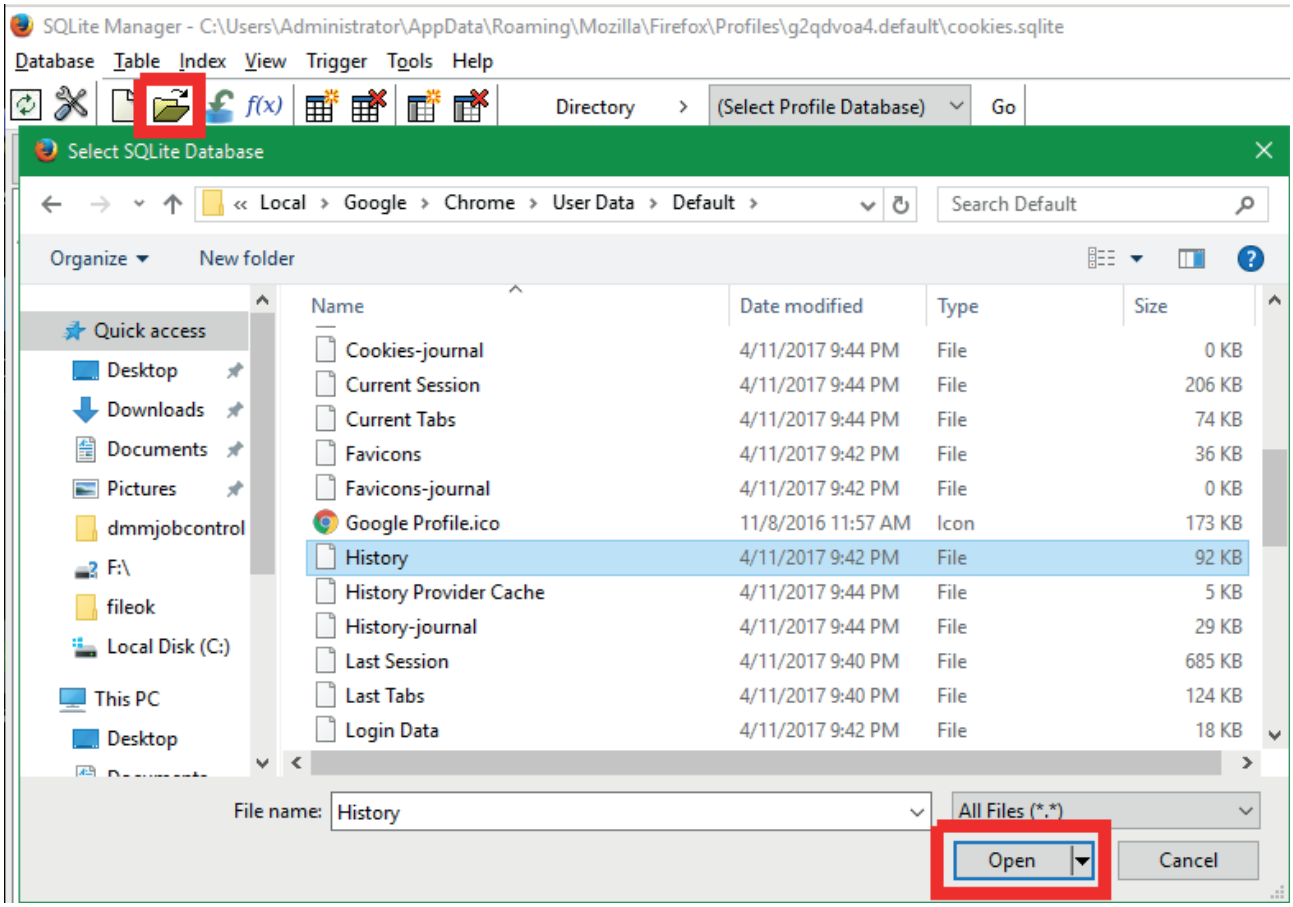
Azonban itt a cache fájloknak mindenféle GUID-os elnevezésük van, ami nehezen használható.

Az eddig használt weboldalról letölthető a PasswordFox alkalmazás, amivel ki tudjuk íratni a jelszavakat. Mint a többi alkalmazásnál, parancssorból is futtatható, ahonnan az eredmény rengeteg formátumban elmenthető, így könnyen felhasználható a végső jelentéshez.

9.5.3. Chrome

A chrome szintén sqlite adatbázisban tárolja az adatokat, ezért analízise hasonló a firefoxhoz.

Az sqlite3 file a következő: vigyázat, nincs kiterjesztése:
C:\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\History
(egyszerűbben, a local user profilon belül Google\Chrome\User Data\<profilnév>\History file)



155. ábra

A chrome sqlite adatbázisának megnyitása

Forrás: A szerző szerkesztése

A két legfontosabb tábla, amire szükségünk van, az urls, ahol megtaláljuk a visit_count oszlopban, hogy hányszor látogatták meg, a typed_count oszlopban, hogy hányszor gépelték be az url mezőben található URL-t. Ha részletesebb adatokra vagyunk kíváncsiak, akkor a visits táblával kell összekötni. Az urls id oszlopa kapcsolódik a visits url oszlopához. A visits táblában részletesen megtaláljuk, mikor látogatták meg az adott URL-t, illetve a transition oszlop megadja, hogyan.

visits
id INTEGER PRIMARY KEY
url INTEGER NOT NULL
visit_time INTEGER NOT NULL
from_visit INTEGER
transition INTEGER DEFAULT 0 NOT NULL
segment_id INTEGER
visit_duration INTEGER DEFAULT 0 NOT NULL

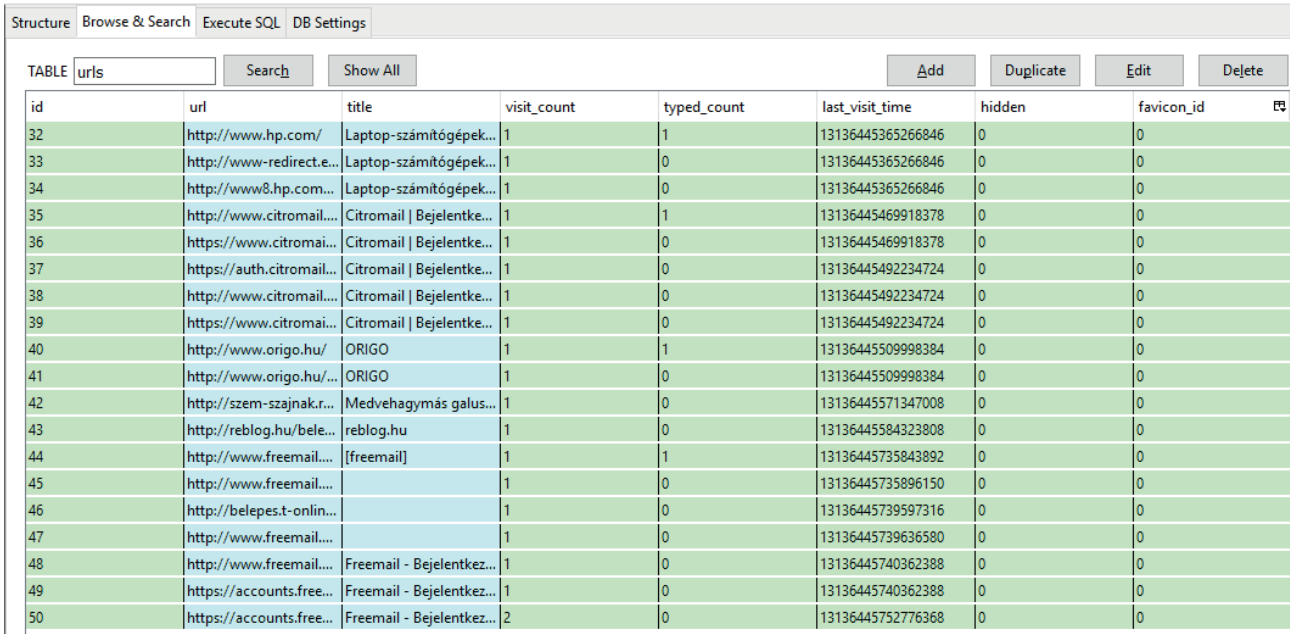
urls
id INTEGER PRIMARY KEY
url LONGVARCHAR
title LONGVARCHAR
visit_count INTEGER DEFAULT 0 NOT NULL
typed_count INTEGER DEFAULT 0 NOT NULL
last_visit_time INTEGER NOT NULL
hidden INTEGER DEFAULT 0 NOT NULL
favicon_id INTEGER DEFAULT 0 NOT NULL

156. ábra

A chrome historyt SQL adatbázisa

Forrás: A szerző saját szerkesztése

Egy példán ez a következőképpen néz ki.



Structure | Browse & Search | Execute SQL | DB Settings

TABLE urls | Search | Show All | Add | Duplicate | Edit | Delete

id	url	title	visit_count	typed_count	last_visit_time	hidden	favicon_id
32	http://www.hp.com/	Laptop-számítógépek...	1	1	13136445365266846	0	0
33	http://www-redirect.e...	Laptop-számítógépek...	1	0	13136445365266846	0	0
34	http://www8.hp.com...	Laptop-számítógépek...	1	0	13136445365266846	0	0
35	http://www.citromail....	Citromail | Bejelentke...	1	1	13136445469918378	0	0
36	https://www.citromai...	Citromail | Bejelentke...	1	0	13136445469918378	0	0
37	https://auth.citromail...	Citromail | Bejelentke...	1	0	13136445492234724	0	0
38	http://www.citromail....	Citromail | Bejelentke...	1	0	13136445492234724	0	0
39	https://www.citromai...	Citromail | Bejelentke...	1	0	13136445492234724	0	0
40	http://www.origo.hu/	ORIGO	1	1	13136445509998384	0	0
41	http://www.origo.hu/...	ORIGO	1	0	13136445509998384	0	0
42	http://szem-szajnak.r...	Medvehagymás galus...	1	0	13136445571347008	0	0
43	http://reblog.hu/bele...	reblog.hu	1	0	13136445584323808	0	0
44	http://www.freemail....	[freemail]	1	1	13136445735843892	0	0
45	http://www.freemail....		1	0	13136445735896150	0	0
46	http://belepes.t-onlin...		1	0	13136445739597316	0	0
47	http://www.freemail....		1	0	13136445739636580	0	0
48	http://www.freemail....	Freemail - Bejelentkez...	1	0	13136445740362388	0	0
49	https://accounts.free...	Freemail - Bejelentkez...	1	0	13136445740362388	0	0
50	https://accounts.free...	Freemail - Bejelentkez...	2	0	13136445752776368	0	0

Structure | Browse & Search | Execute SQL | DB Settings

TABLE visits | Search | Show All | Add | Duplicate | Edit | Delete

id	url	visit_time	from_visit	transition	segment_id	visit_duration
32	32	13136445365266846	0	268435457	1	0
33	33	13136445365266846	32	-2147483647	0	0
34	34	13136445365266846	33	-1610612735	0	94583330
35	35	13136445469918378	0	268435457	2	0
36	36	13136445469918378	35	-1610612735	0	0
37	37	13136445492234724	0	268435463	0	0
38	38	13136445492234724	37	-2147483641	0	0
39	39	13136445492234724	38	-1610612729	0	9964774
40	40	13136445509998384	0	268435457	3	0
41	41	13136445509998384	40	-1610612735	0	61348624
42	42	13136445571347008	41	805306368	3	12976800
43	43	13136445584323808	42	805306368	3	0
44	44	13136445735843892	0	838860801	4	0
45	45	13136445735896150	44	1610612736	0	0
46	46	13136445739597316	45	1610612736	0	0
47	47	13136445739636580	46	1610612736	0	0
48	48	13136445740362388	47	1073741824	0	0
49	49	13136445740362388	48	-2147483648	0	0
50	50	13136445740362388	49	-1610612736	0	0
51	50	13136445752776368	0	805306375	0	0

157. ábra

A chrome sqlite adatbázisa

Forrás: A szerző szerkesztése

A transition oszlop jelentéseit úgy találjuk meg, hogy rákeresünk a page_transition_types.h fájlra az interneten. Ez valamivel bonyolultabb, mint a firefox esetében volt, itt a legalsó és a legfelső bytenak vannak jelentései, és azok kombinálódnak a végső transition értékhez. Sőt, a legfelső byte akár egyszerre több érték is lehet.

4. táblázat

A chrome sqlite értelmezése

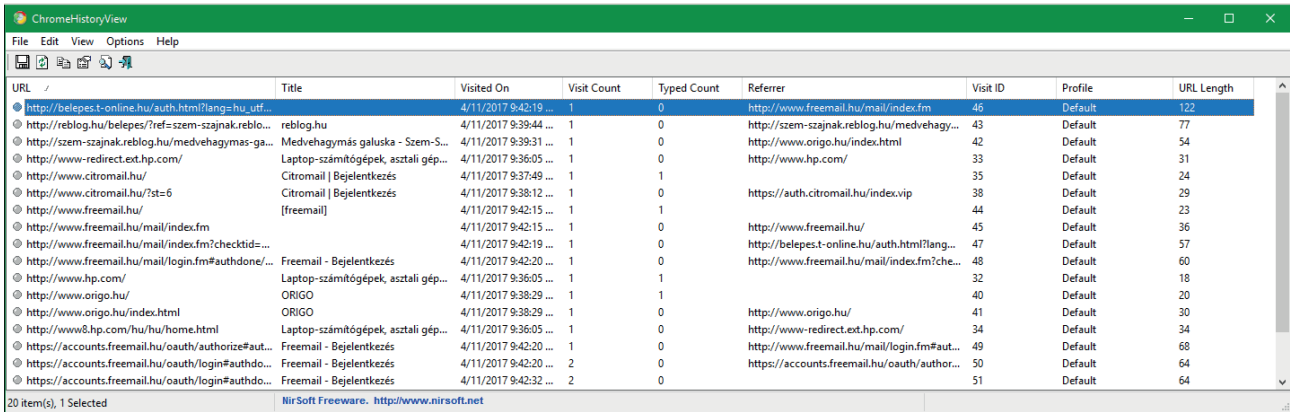
value	name	description
0x00	LINK	User got to this page by clicking a link on another page
0x01	TYPED	typing the URL in the URL bar or other "explicit" navigation actions.
0x02	AUTO_BOOKMARK	a suggestion in the UI
0x03	AUTO_SUBFRAME	Automatcally loaded in a non-toplevel frame, user may not even realize the content in these pages is a separate frame, so may not care about the URL
0x04	MANUAL_SUBFRAME	subframe navigations that are explicitly requested by the user, generate new navigation entries in the back/forward list. user probably cares about the fact that this link was loaded.
0x05	GENERATED	typing in the URL bar and selecting an entry that did not look like a URL. For example, a match might have the URL of a Google search result page, but appear like "Search Google for ...". These are not quite the same as TYPED navigations because the user didn't type or see the destination URL.
0x06	START_PAGE	page was specified in the command line or is the start page.
0x07	FORM_SUBMIT	The user filled out values in a form and submitted it. NOTE that in some situations submitting a form does not result in this transition type. This can happen if the form uses script to submit the contents.
0x08	RELOAD	user "reloaded" the page, either by hitting the reload button or by hitting enter in the address bar.
0x09	KEYWORD	The url was generated from a replaceable keyword other than the default search provider. If the user types a keyword (which also applies to tab-to-search) in the omnibox this qualifier is applied to the transition type of the generated url. TemplateURLModel then may generate an additional visit with a transition type of KEYWORD_GENERATED against the url 'http://' + keyword. For example, if you do a tab-to-search against wikipedia the generated url has a transition qualifer of KEYWORD, and TemplateURLModel generates a visit for 'wikipedia.org' with a transition type of KEYWORD_GENERATED.
0x10	KEYWORD_GENERATED	Corresponds to a visit generated for a keyword.
0x01000000	FORWARD_BACK	Forward or Back button to navigate among browsing history.
0x02000000	FROM_ADDRESS_BAR	User used the address bar to trigger this navigation.
0x04000000	HOME_PAGE	User is navigating to the home page.
0x10000000	CHAIN_START	beginning of a navigation chain.
0x20000000	CHAIN_END	last transition in a redirect chain.
0x40000000	CLIENT_REDIRECT	Redirects caused by JavaScript or a meta refresh tag on the page.
0x80000000	SERVER_REDIRECT	Redirects sent from the server by HTTP headers.

Forrás: A szerző saját szerkesztése

Természetesen léteznek automata toolok is ezeknek az információknak a kiszedésére, de vigyázzunk, ezek általában nem adnak meg annyi részletet, mintha közvetlenül SQL-el kérdezzük le az adatbázist. Például sok esetben az automata toolok jelentései nem tartalmazzák a transition-ot, ezért fontos tudnunk, hogy manuálisan hol találjuk ezeket az információkat, és hogyan tudjuk kinyerni őket.

Az egyik legelterjedtebb browser history-t listázó eszköz a www.nirsoft.net-ről letölthető ChromeHistoryView. Ez grafikusan nagyon szépen összeszedi a látogatott weboldalakat, de parancssorból is futtathatjuk, és akkor lehetőség van az eredmény fájlba mentésére nagyon sokféle formátumban, amit utána könnyen illeszthetünk a jelentésünkbe.

Amikor elindítjuk az alkalmazást, automatikusan kigyűjti az aktuális user history-ját.

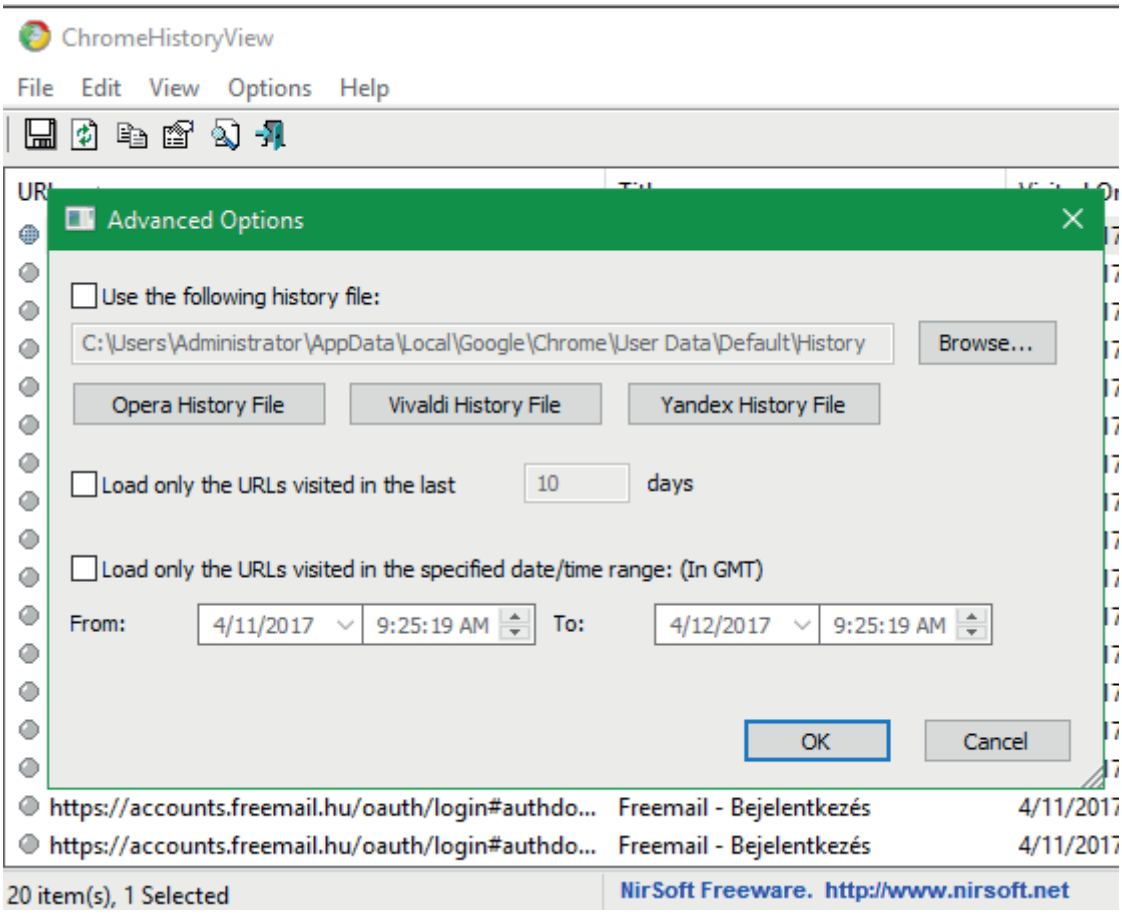


158. ábra

A ChromeHistoryView alkalmazás

Forrás: A szerző szerkesztése

Amennyiben például egy diskimage-dzsel dolgozunk, meg kell adni az elérési útját a historyfájlnak, ezt az options / advanced options menüponttal tudjuk megtenni.



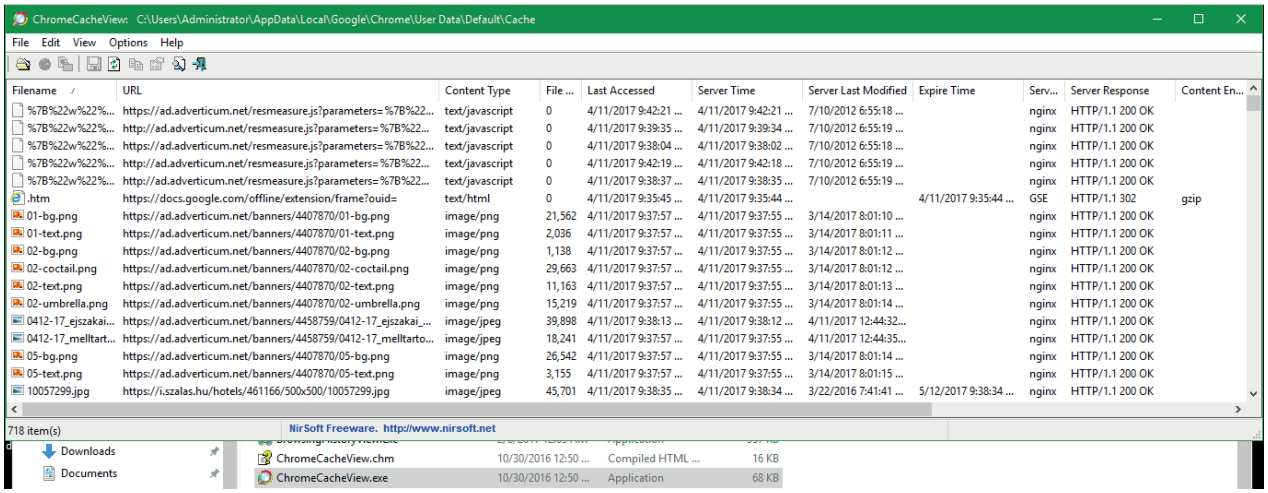
159. ábra

A historyfájl elérési útjának megadása

Forrás: A szerző szerkesztése

Érdemes megvizsgálni a cache tartalmát, ahol a meglátogatott weboldalakról szerezhetünk információt. Csakúgy, mint máskor, egyszerűbb, ha automata toolokkal próbálkozunk. A korábban már használt

www.nirsoft.net weboldalon találjuk a ChromeCacheView alkalmazást, ami megmutatja nekünk a cache tartalmát. Ahogy a többi alkalmazásnál, parancssorból is futtatható, ahonnan az eredmény rengeteg formátumban elmenthető, így könnyen felhasználható a végső jelentéshez.

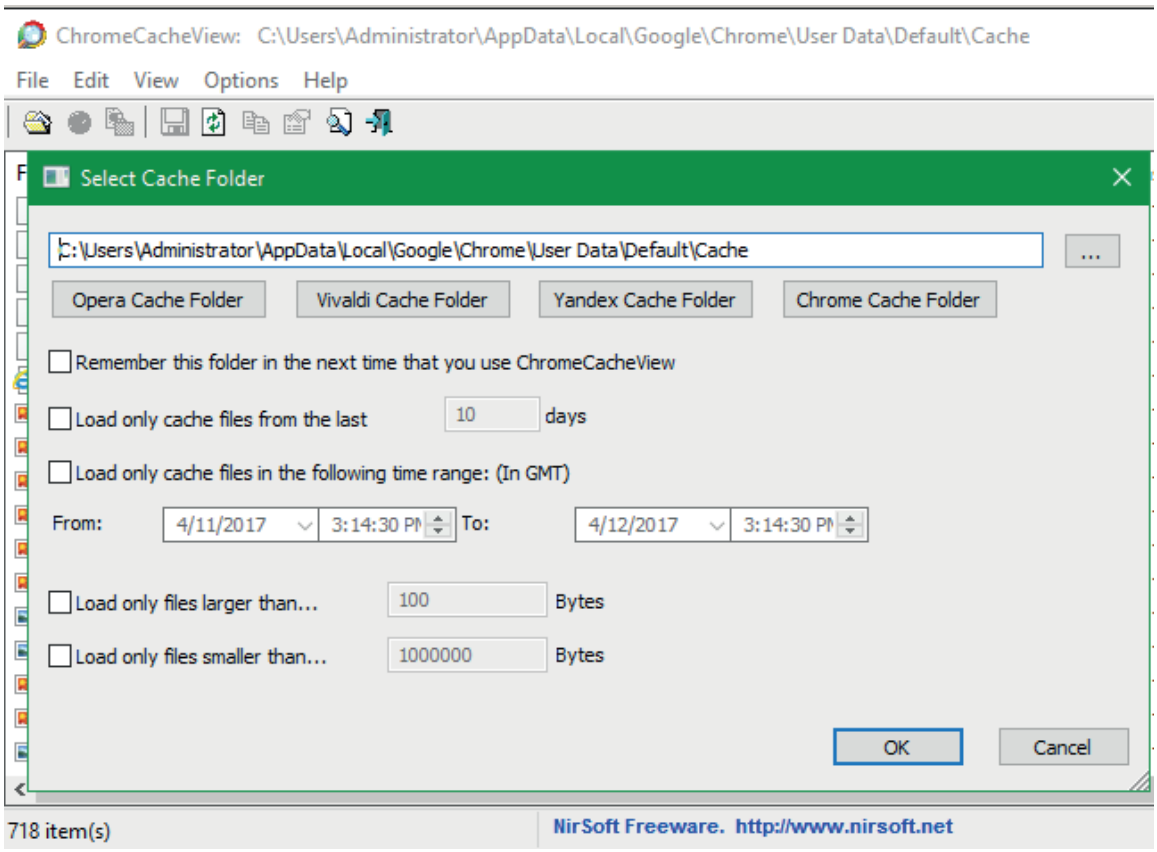


160. ábra

A ChromeCacheView alkalmazás használata

Forrás: A szerző szerkesztése

Következő lépés, a File / select cache folder lehetőségre kattintás.



161. ábra

A cache kiválasztása

Forrás: A szerző szerkesztése

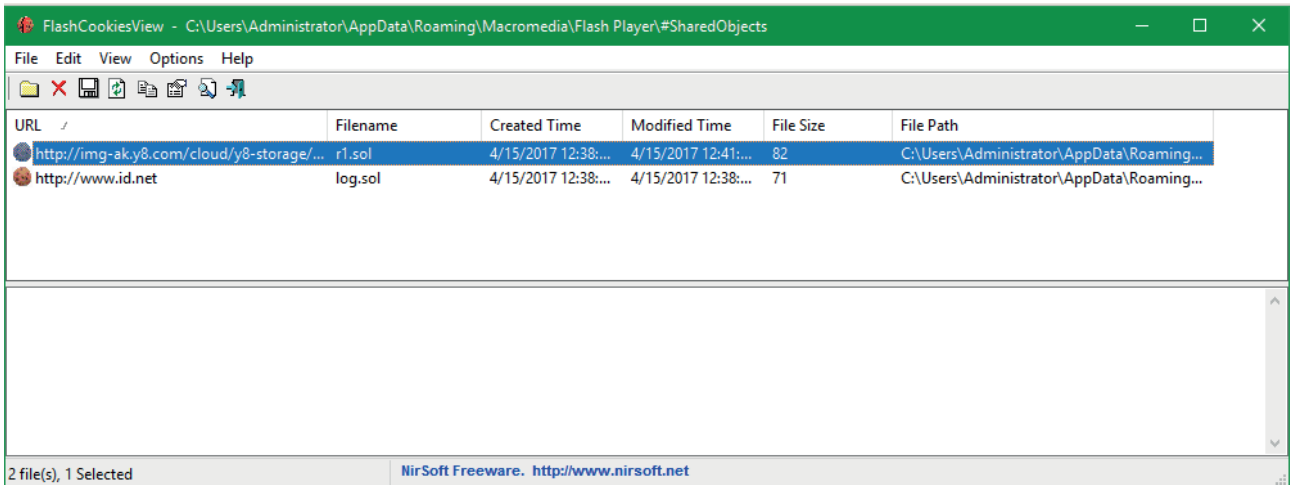
Amennyiben valaki manuálisan szeretné megvizsgálni a cookie-kat, annak helye:
C:\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Cache
(egyszerűbben, a local user profilon belül Google\Chrome\User Data\<profilnév>\Cache alkönyvtár)

Ahogy a többi böngészőnél, itt is keressünk letárolt jelszavakat a már ismertetett elvek alapján. Az eddig használt weboldalról letölthető a ChromePass alkalmazás, amivel ki tudjuk íratni a jelszavakat. Ahogy a többi alkalmazásnál, ez is parancssorból is futtatható, ahonnan az eredmény rengeteg formátumban elmenthető, így könnyen felhasználható a végső jelentéshez.

9.5.4. Flash

Szerencsére már kihalóban van a flash, sötét korszaka volt a weboldalak biztonságának. De azért még előfordulhatnak ilyenek. Ma már sok felhasználó tisztában van azzal, hogy törölni kell a cookiekat, böngésző historyt és hasonlókat, de azzal nagyon kevesen vannak tisztában, hogy a flash-nek saját history-ja és cache-e van. Ezért, különösen, olyan esetekben, ha a böngészők adatait törölték, megpróbálhatjuk a flashadatokat megnézni.

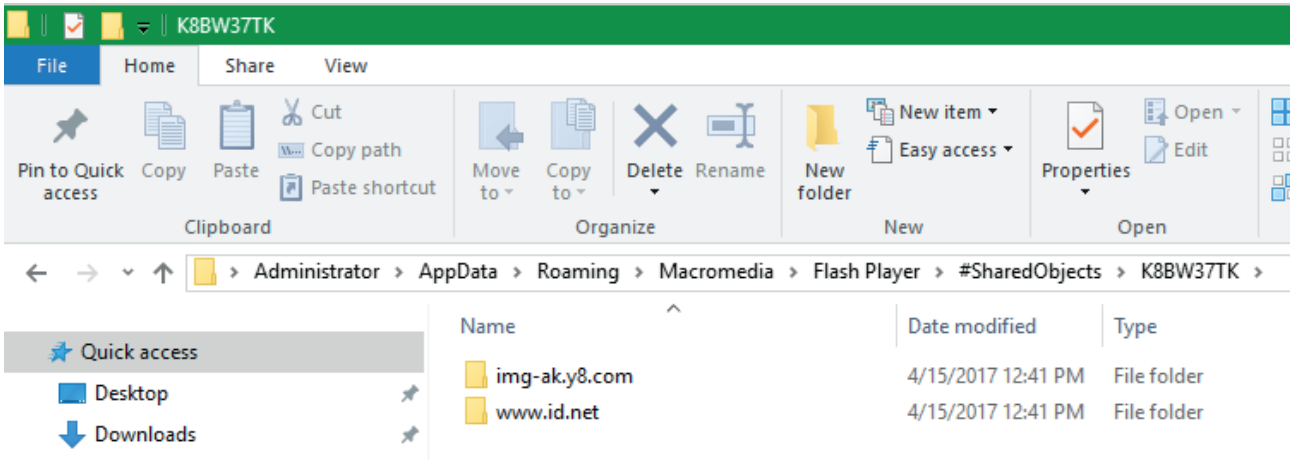
Ezt egyszerűbb automata toolokkal ellenőrizni, szintén a www.nirsoft.net weboldalról tölthető le a flashcookiesview.



162. ábra
A flashcookiesview alkalmazás

Forrás: A szerző szerkesztése

De ha manuálisan szeretnénk megkeresni, a flashcache a következő helyen található:
C:\Users\Administrator\AppData\Roaming\Macromedia\Flash Player\#SharedObjects



163. ábra

A flashcache helye

Forrás: A szerző szerkesztése

9.6. E-mailek vizsgálata

E-mailek vizsgálatánál szintén nem számít, milyen operációs rendszerről származnak maguk az adatfájlok. Én a legelterjedtebb, outlook formátumot mutatom meg. Outlook esetében ost, illetve pst a két fájltípus, amivel találkozhatunk.

9.6.1. OST, PST fájlok

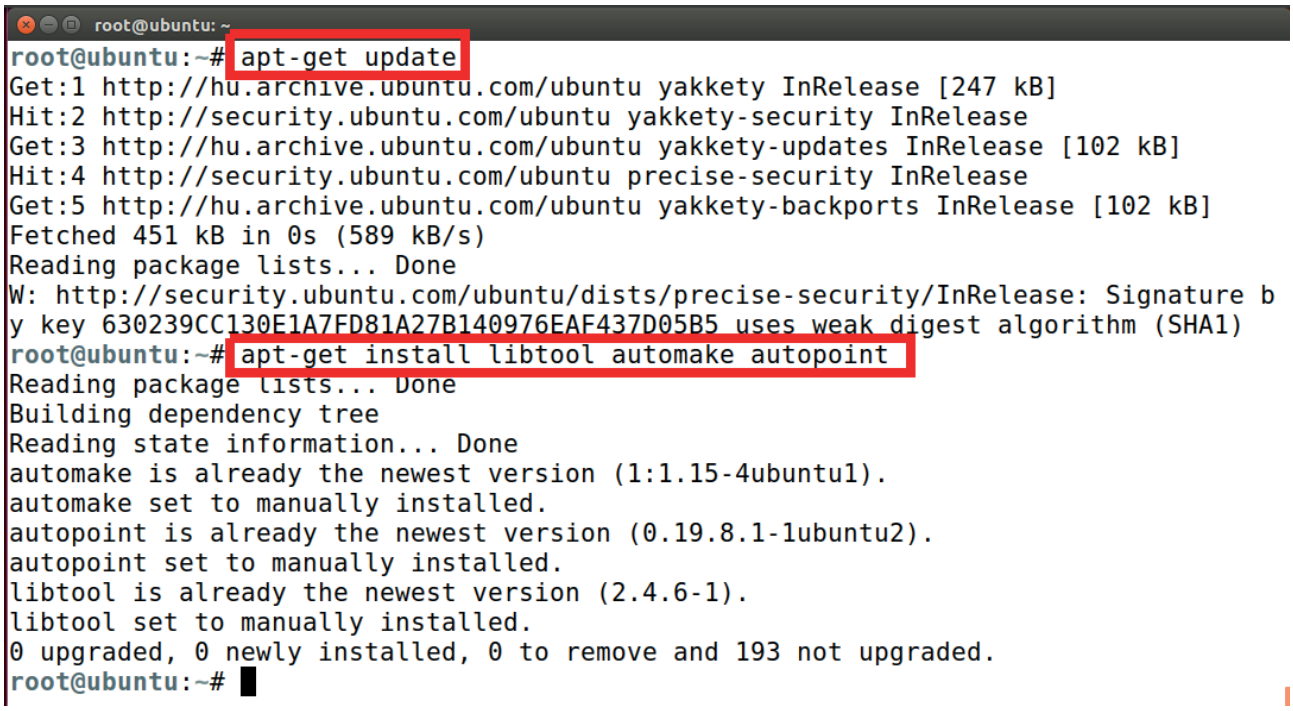
A két formátum kezelése közül a .pst az egyszerűbb. Egyszerű megoldásként akár saját outlookba is becsatolhatjuk és olvashatjuk a leveleket. Ilyenkor természetesen vigyázzunk, hogy a gép, ahová becsatoljuk, semmilyen körülmények között ne legyen internetre csatlakoztatva, mert lehetnek beragadt e-mailek. Természetesen ez ebben az esetben sem a legjobb megoldás, inkább csak a gyors, kényelmes áttekintéshez jó. Hátrányai a módszernek, hogy nem mutatja a lomtárból is törölt elemeket. A pst és ost fájlok adatbázisfájlok, amikor törlünk, akár véglegesen is, nem törlődnek az elemek, hanem csak bejegyződik, hogy törölt. A fájlból csak annak kompaktálásával lehet ezeket eltüntetni, amit nagyon kevés felhasználó csinál.

Másik problémát a titkosított pst fájlok okozzák. Szerencsére ez valójában nem probléma, mivel a .pst titkosítása nagyon gyenge. Úgy működik, hogy a pst fájl tartalmát egy fix kulccsal titkosítja, majd ezt a fix kulcsot titkosítja a mi jelszavunkkal. Ez még alapvetően nem lenne rossz, hasonlóan működik a pgp és az EFS is, egy fix szimmetrikus kulccsal titkosítja az adatot, és ezt a szimmetrikus kulcsot titkosítja le. De ezek minden esetben más-más fix kulcsot használnak, míg a pst minden esetben ugyanazt a kulcsot használja a világ összes pst-jében, nem generál újat. Emiatt, ha ismerjük ezt a fix kulcsot, ki tudjuk bontani a pst fájl tartalmát a jelszó ismerete nélkül is, márpedig nyilván csak idő kérdése volt, hogy kiderüljön.

A következő probléma az ost fájlok tartalma, amelyeket nem tudunk egy outlookba becsatolni, hiszen ezek gyakorlatilag temp fájlok.

Amennyiben az előbb leírt gondjaink adódnak, más megoldásra van szükség. Az interneten lehet ost, pst nézegetőket találni, nagyságrendileg pár száz dolláros áron. Amennyiben ingyenes megoldást szeretnénk, akkor a libpff használata ajánlott. Ez egy ingyenes linuxos alkalmazás, kifejezetten ost, pst fájlok kezelésére és kibontására írva. Ezt forrásból tudjuk telepíteni.

Ellenőrizzük, hogy az automake-hez szükséges csomagok telepítve vannak-e, ha nem, akkor telepítsük őket az apt-get update és/vagy az apt-get install libtool automake autopoint használatával.

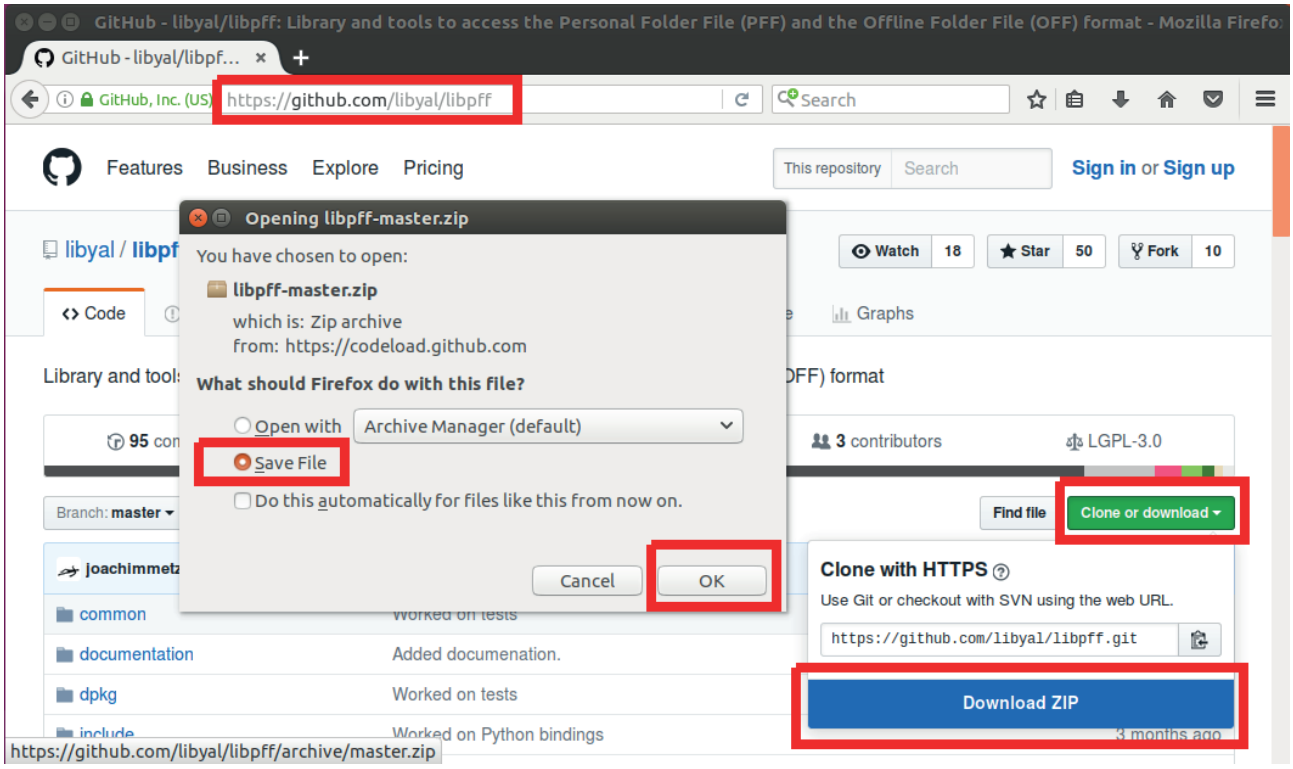


164. ábra

A libpff telepítése

Forrás: A szerző szerkesztése

Töltsük le a libpff libraryt a githubról (https://github.com/libyal/libpff).



165. ábra

A libpff library letöltése

Forrás: A szerző szerkesztése

Lépjünk be az alkönyvtárba, ahová letöltöttük, majd bontsuk ki unzip paranccsal, amit leszedtünk.

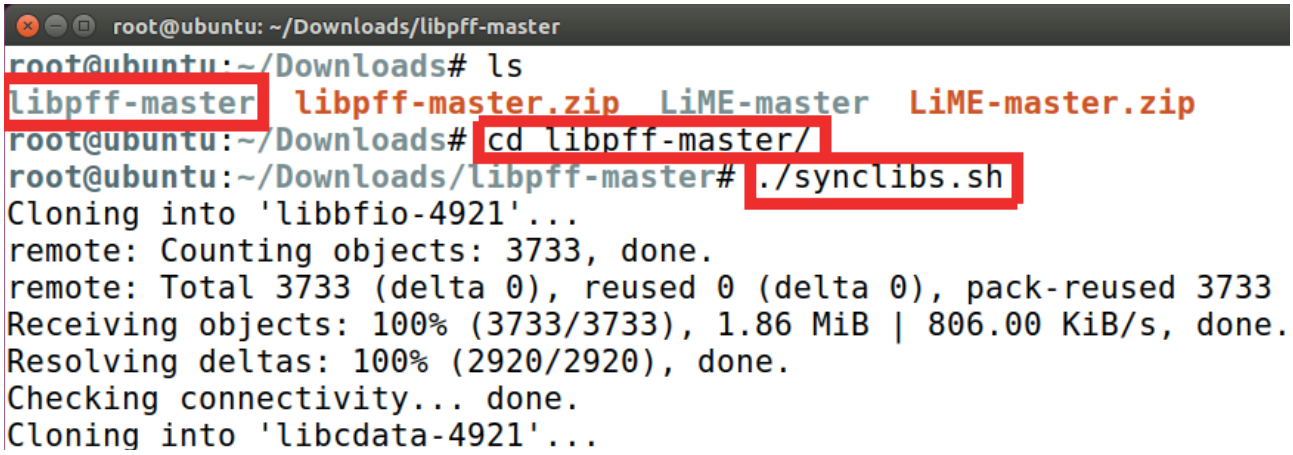
```
root@ubuntu: ~/Downloads
root@ubuntu:~# cd Downloads/
root@ubuntu:~/Downloads# ls
libpff-master.zip  LiME-master  LiME-master.zip
root@ubuntu:~/Downloads# unzip libpff-master.zip
Archive:  libpff-master.zip
887db28dd06d721c0029f3ebbbab6d55db132514
   creating: libpff-master/
  inflating: libpff-master/.codecov.yml
  inflating: libpff-master/.gitignore
```

166. ábra

A libpff library kicsomagolása

Forrás: A szerző szerkesztése

Ezután szedjük le a libraryhoz szükséges thirdparty csomagokat: ./synclibs.sh

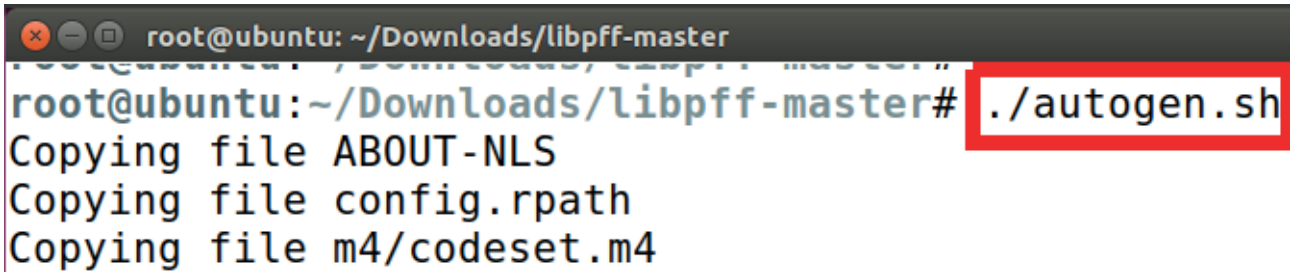


167. ábra

A szükséges thirdparty csomagok leszedése

Forrás: A szerző szerkesztése

Majd generáljuk le a szükséges fájlokat: ./autogen.sh

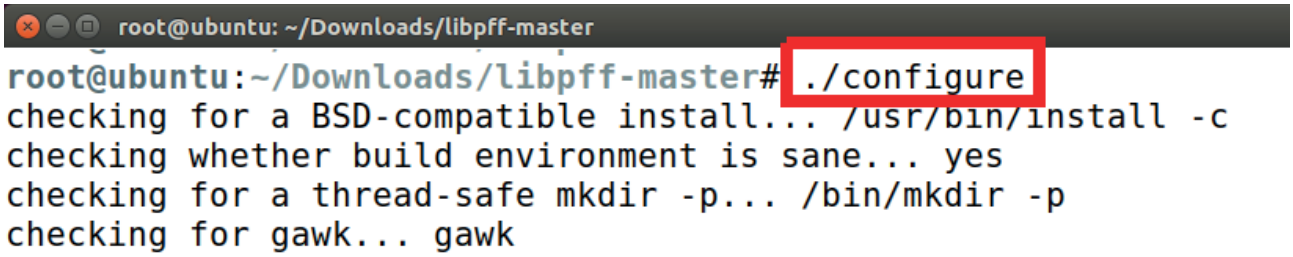


168. ábra

A szükséges fájlok legenerálása

Forrás: A szerző szerkesztése

Innentől jön a szokásos linuxos fordítás, a ./configure, hogy beállítsuk a paramétereket.



169. ábra

A paraméterek beállításához szükséges fordítás

Forrás: A szerző szerkesztése

Ezután fordítsuk le a make paranccsal!

```
root@ubuntu: ~/Downloads/libpff-master
root@ubuntu:~/Downloads/libpff-master#
root@ubuntu:~/Downloads/libpff-master# make
Making all in include
make[1]: Entering directory '/home/administrator/Downloads/libpff-master/include'
make[1]: Nothing to be done for 'all'.
make[1]: Leaving directory '/home/administrator/Downloads/libpff-master/include'
Making all in common
```

170. ábra

A linuxos fordítás indítása

Forrás: A szerző szerkesztése

Végezetül telepítsük a make install paranccsal!

```
root@ubuntu: ~/Downloads/libpff-master
root@ubuntu:~/Downloads/libpff-master# make install
Making install in include
make[1]: Entering directory '/home/administrator/Downloads/libpff-master/include
'
make[2]: Entering directory '/home/administrator/Downloads/libpff-master/include
'
```

171. ábra

A telepítés indítása

Forrás: A szerző szerkesztése

A fordítás .so fájlokat is készít (shared object, olyasmi, mint a windowsos rendszereken a dll fileok), amelyeket azonban regisztrálni kell, másképpen nem találja az operációs rendszer, ezért használjuk az ldconfig parancsot, ezután már működnek az új parancsok mint pffexport.

```
root@ubuntu: ~/Downloads/libpff-master
root@ubuntu:~/Downloads/libpff-master# pffexport
pffexport: error while loading shared libraries: libpff.so.1: cannot open shared
 object file: No such file or directory
root@ubuntu:~/Downloads/libpff-master# ldconfig
root@ubuntu:~/Downloads/libpff-master# pffexport
pffexport 20170115

Missing source file.
Use pffexport to export items stored in a Personal Folder File (OST, PAB
and PST).

Usage: pffexport [ -c codepage ] [ -f format ] [ -l logfile ] [ -m mode ]
                 [ -t target ] [ -dhqvV ] source

        source: the source file
```

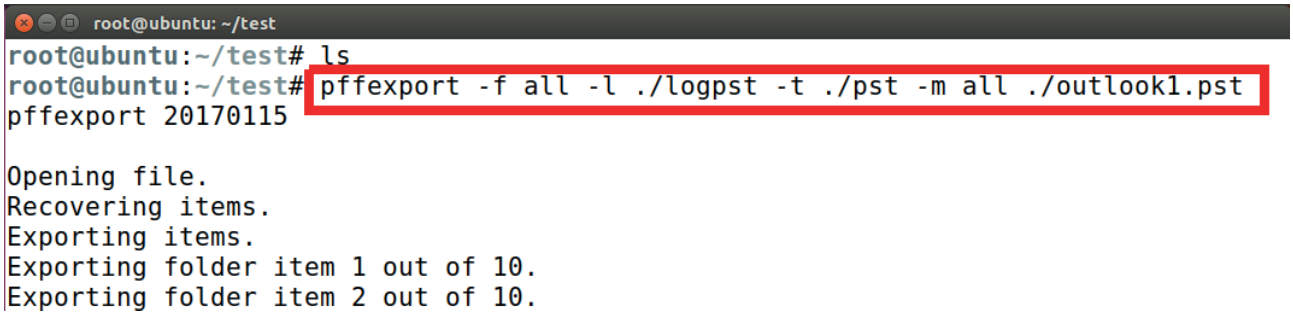
172. ábra

Az ldconfig parancs használata

Forrás: A szerző szerkesztése

Ezek után kibonthatjuk a pst és ost fájlok tartalmát; első példa egy egyszerű pst fájl:

pffexport -f all -l ./logpst -t ./pst -m all ./outlook1.pst

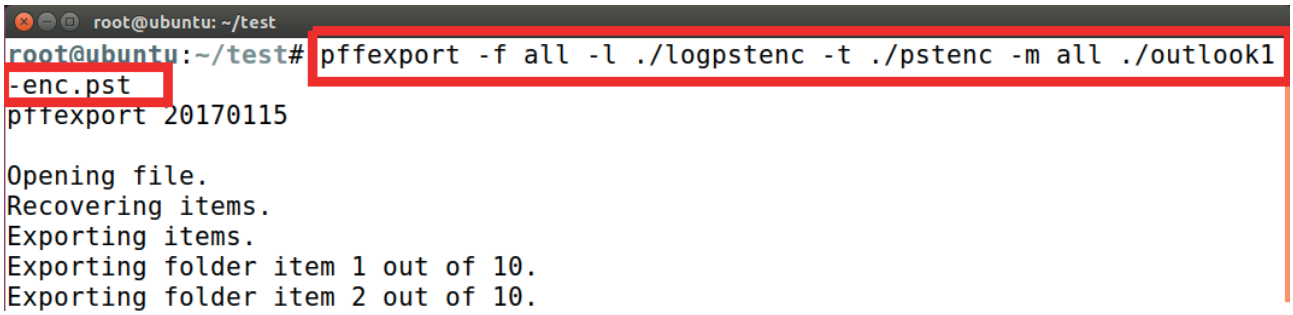


173. ábra

Egy pst fájl tartalmának kibontása

Forrás: A szerző szerkesztése

Titkosított pst kibontása semmiben nem különbözik egy sima pst fájl kibontásától: pffexport -f all -l ./logpstenc -t ./pstenc -m all ./outlook1-enc.pst



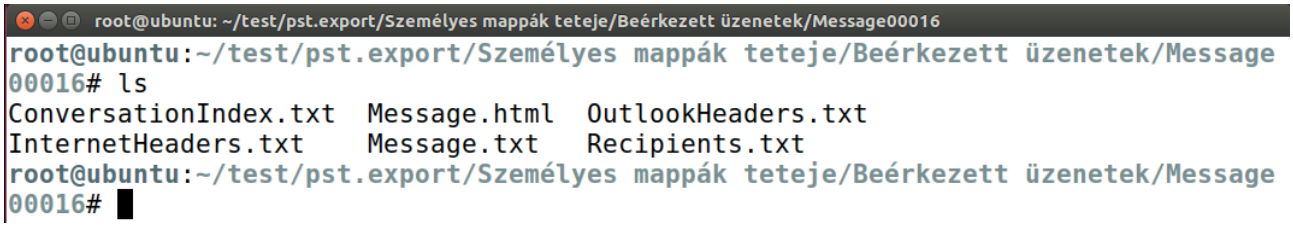
174. ábra

Titkosított pst fájl kibontása

Forrás: A szerző szerkesztése

Az ost fájlok kibontása szintén megegyezik egy sima pst fájl kibontásával: pffexport -f all -l ./logost -t ./ost -m all ./outlook1.ost

A kibontott fájlok egy alkönyvtárszerkezetbe kerülnek, ami hasonló az outlookban látható mappákhoz.



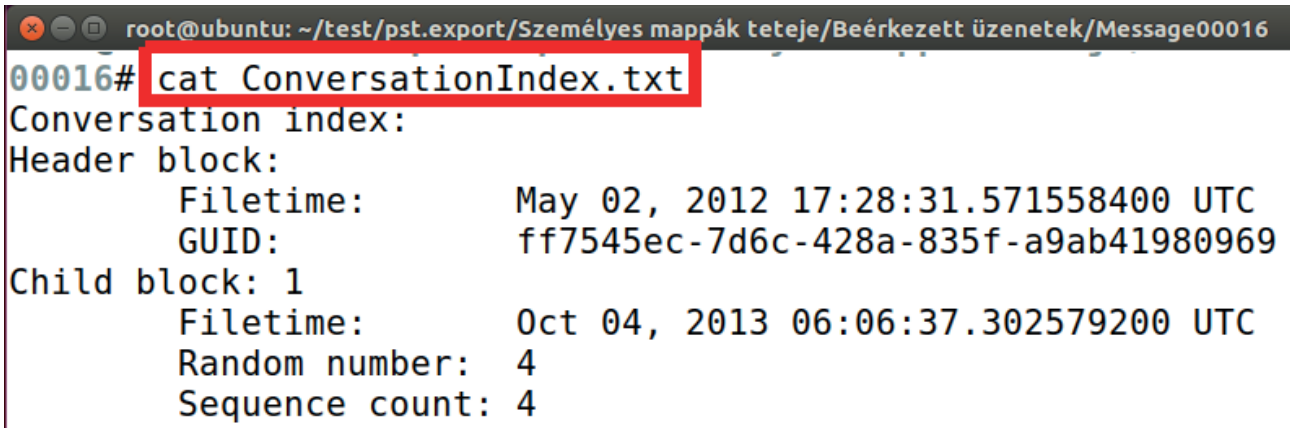
175. ábra

A kibontott fájlok helye

Forrás: A szerző szerkesztése

Amikor belépünk egy üzenetet tartalmazó mappába, több fájlt találunk. A Message.xxx az e-mail tartalma. Amennyiben a levélben volt csatolmány is, akkor van egy csatolány alkönyvtár, amiben azokat találjuk.

A conversationindex.txt fájlban az e-mail fontosabb alapadatait találjuk, mint a hozzá rendelt egyedi azonosító, amivel például a szerver logban beazonosíthatjuk.

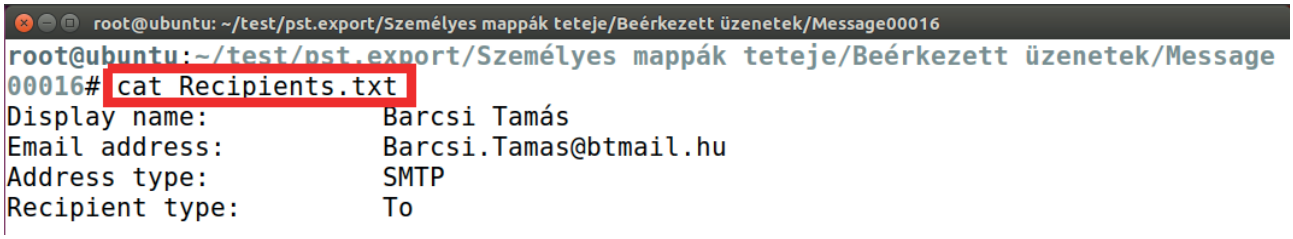


176. ábra

Az e-mail fontosabb alapadatait tartalmazó conversationindex.txt fájl

Forrás: A szerző szerkesztése

A Recipients.txt-ben a címzettek különböző nevei olvashatók.

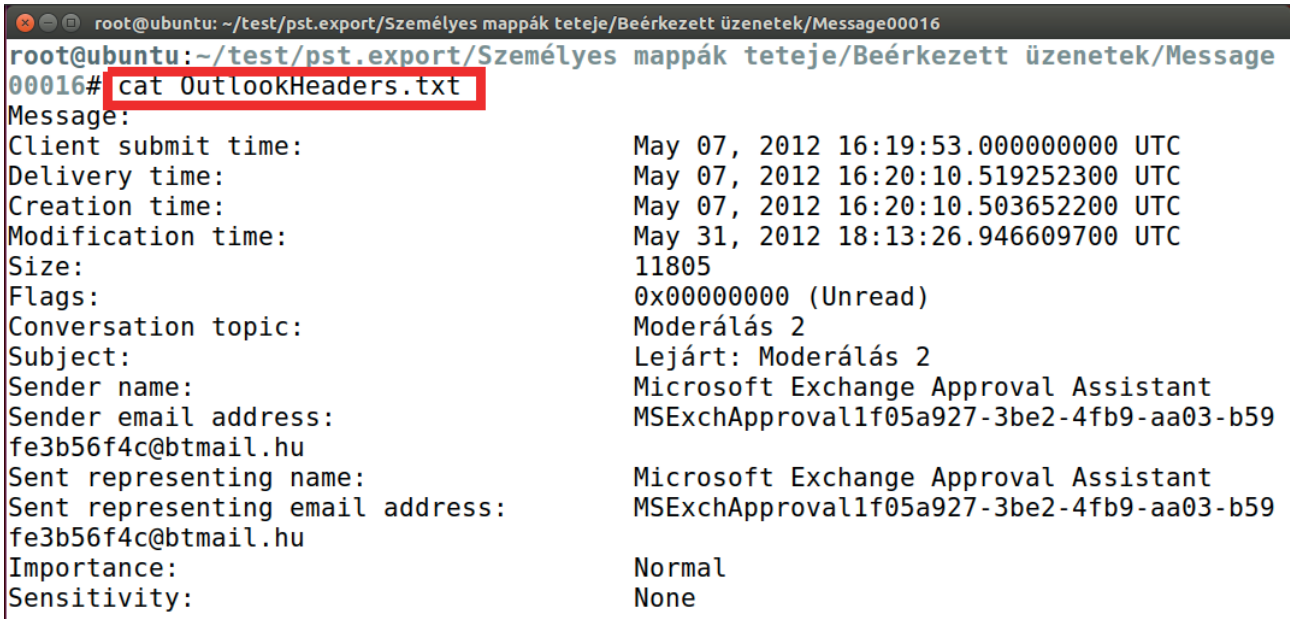


177. ábra

A recipients.txt-ben olvasható címzettek

Forrás: A szerző szerkesztése

Az OutlookHeaders-ben a vannak az e-mail metaadatai, küldés, fogadás ideje, flagek (például olvasott/olvasatlan).

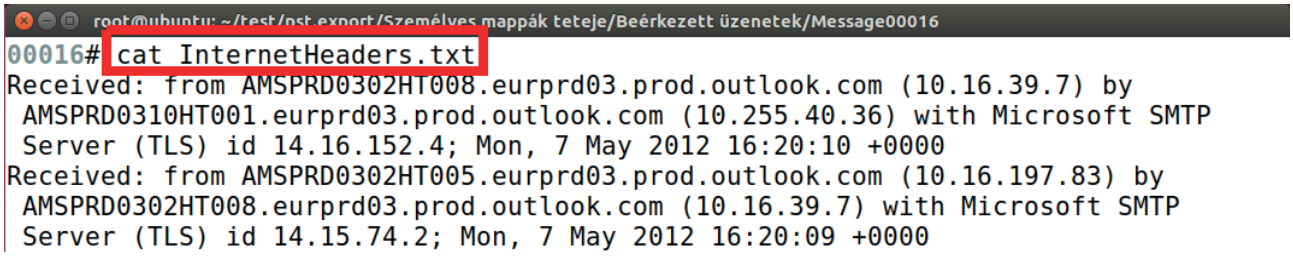


178. ábra

Az e-mail metaadatait tartalmazó Outlookheaders.txt

Forrás: A szerző szerkesztése

Az InternetHeaders.txt-ben van az amit, e-mail-headernek szoktunk nevezni. Itt lehet megtalálni, hogy milyen SMTP szervereken utazott keresztül az e-mail, itt kapunk némi információt a feladó IP-céméről.

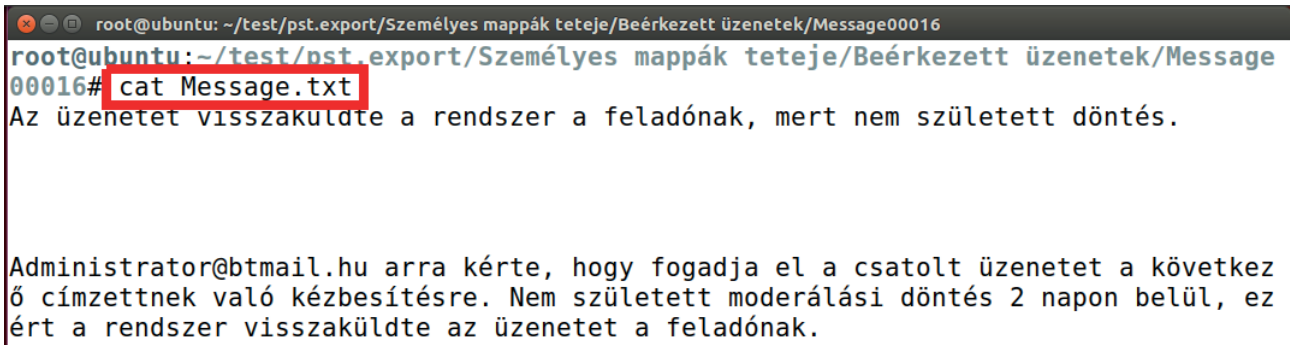


179. ábra

E-mail-header

Forrás: A szerző szerkesztése

És végezetül a Message nevű fájlokban van az üzenet, különböző formátumokban.



180. ábra

A message nevű fájl

Forrás: A szerző szerkesztése

A pst.export mellett van még egy pst.recovered nevű alkönyvtár is, ahol a visszaállított törölt fájlokat találjuk.

A többi fájl esetében is hasonló könyvtár szerkezetet kapunk és hasonlóan tudjuk kezelni. Mivel potenciálisan rengeteg e-mail van egy pst fájlban, akár százezres nagyságrendben, tipikusan kulcsszavas keresést szoktunk indítani a kapott alkönyvtárszerkezetre, hogy megtaláljuk a nekünk érdekeseket, és azokkal foglalkozzunk részletesebben.

Az OST és a PST fájlok hivatalos és részletes leírása itt található meg:
http://msdn.microsoft.com/en-us/library/ff385210.aspx

9.7. Logok vizsgálata

Természetesen sok hasznos információ található a logfájlokban is. Elsősorban a ki- és bejelentkezések időpontjai, amit itt keresünk.

Logokból rengetegféle van, operációs rendszerverziónként is el tudnak térni. Illetve másik probléma, hogy hogyan van beállítva a logolás, ez alapvetően meghatározza, mit találhatunk meg a logokban.

Az operációs logon kívül az egyes alkalmazások logjai is fontosak, de tekintetbe véve, hogy milyen sok alkalmazás van, és azoknak milyen sok verziója, az alkalmazásokat mindig egyedileg kell megvizsgálni.

9.7.1. Windows operációs rendszerek logjai

Windows esetében alapvetően kétfajta logolást különböztetünk meg, az egyik a klasszikus, amely alapértelmezés szerint be van kapcsolva, a másik a 2012-ben bevezetett advanced audit policy, amelyet külön kell aktiválni, de sokkal részletesebb logolást tesz lehetővé. Sajnos a hivatalos dokumentáció nem elég részletes, például nem tér ki a bejelentkezések típusaira (SMB, Remote Desktop, FTP, IIS, lokális), csak nagy vonalakban emlegeti a belépést.

Az alapvető kérdés, amire választ szoktunk keresni, hogy ki(k) volt(ak) belépve egy adott időpontban. Erre az egyszerűnek tűnő kérdésre valójában elég nehéz válaszolni. A számítógépen ugyanis rengeteg automatikus folyamat fut, amelyek induláskor belépéslogot, leálláskor pedig kilépéslogot generálnak. Ilyenek például a frissítési folyamatok.

Magánál a belépési folyamatnál nemcsak egy logbejegyzés keletkezik, hanem számos. Ezek között rengeteg null session-ös bejelentkezés.

Azt, hogy melyik logonfolyamatnak melyik logoff a párja, a logonidparaméter segítségével tudjuk összerendelni. Ebből vonhatunk le következtetést, hogy ki(k) az(ok), aki(k) éppen be volt(ak) jelentkezve egy adott időpontban.

Nézzünk példaképpen egy bejelentkezési folyamatot!

A folyamat számunkra leginkább fontos része egy 4776-os Credential Validation eseménnyel indul.

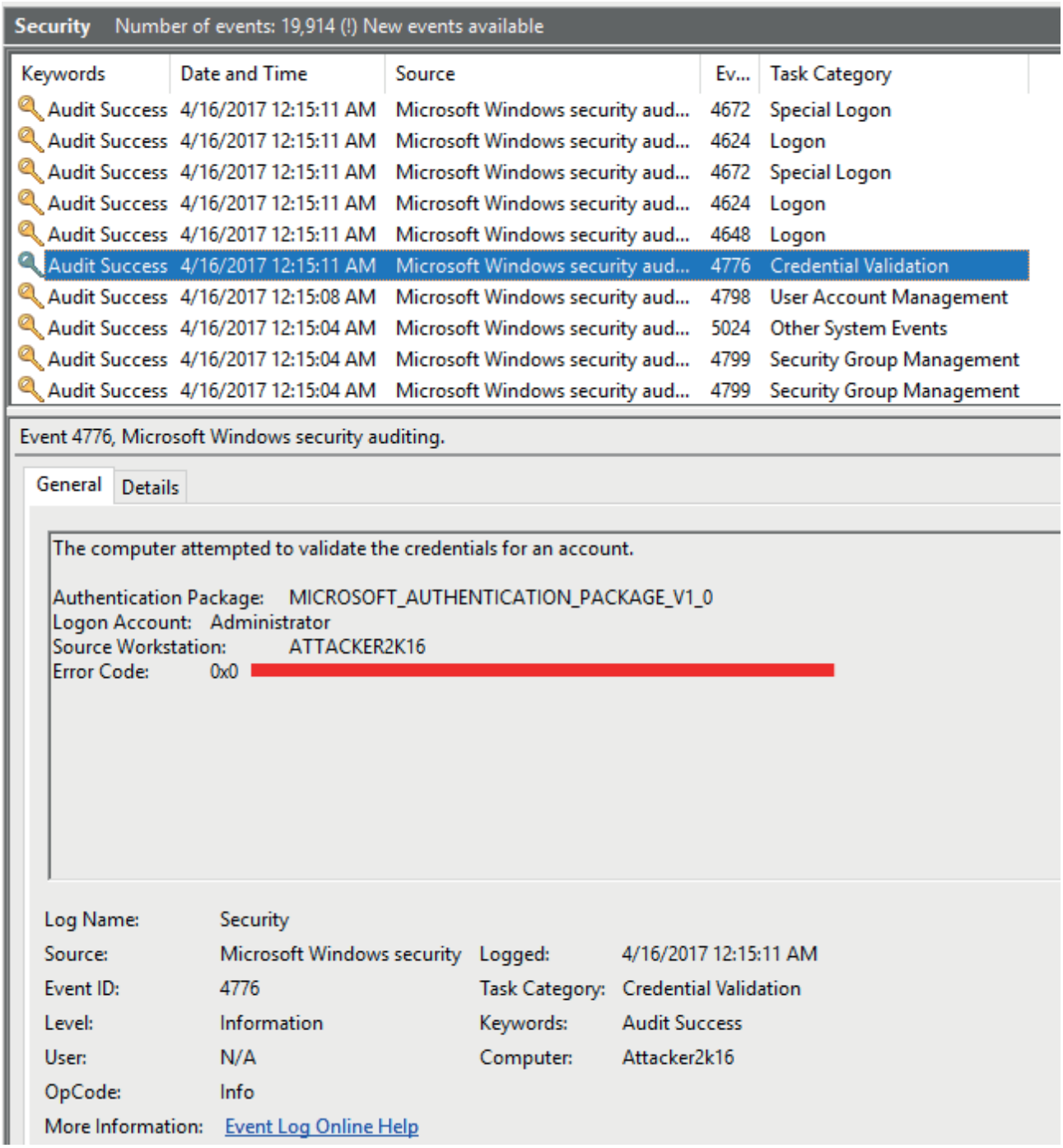
Itt a logon account paraméterből megtuthatjuk, hogy ki akart bejelentkezni; jelen pillanatban az administrator nevű felhasználó.

És az error code paraméterből, hogy sikerült-e az authentikáció, vagyis helyes volt-e a jelszó. A 0 jelenti, hogy igen, sikeres.

5. táblázat
Az error code táblázat

error code	description
C0000064	user name does not exist
C000006A	user name is correct but the password is wrong
C0000234	user is currently locked out
C0000072	account is currently disabled
C000006F	user tried to logon outside his day of week or time of day restrictions
C0000070	workstation restriction
C0000193	account expiration
C0000071	expired password
C0000224	user is required to change password at next logon
C0000225	evidently a bug in Windows and not a risk

Forrás: msdn.com

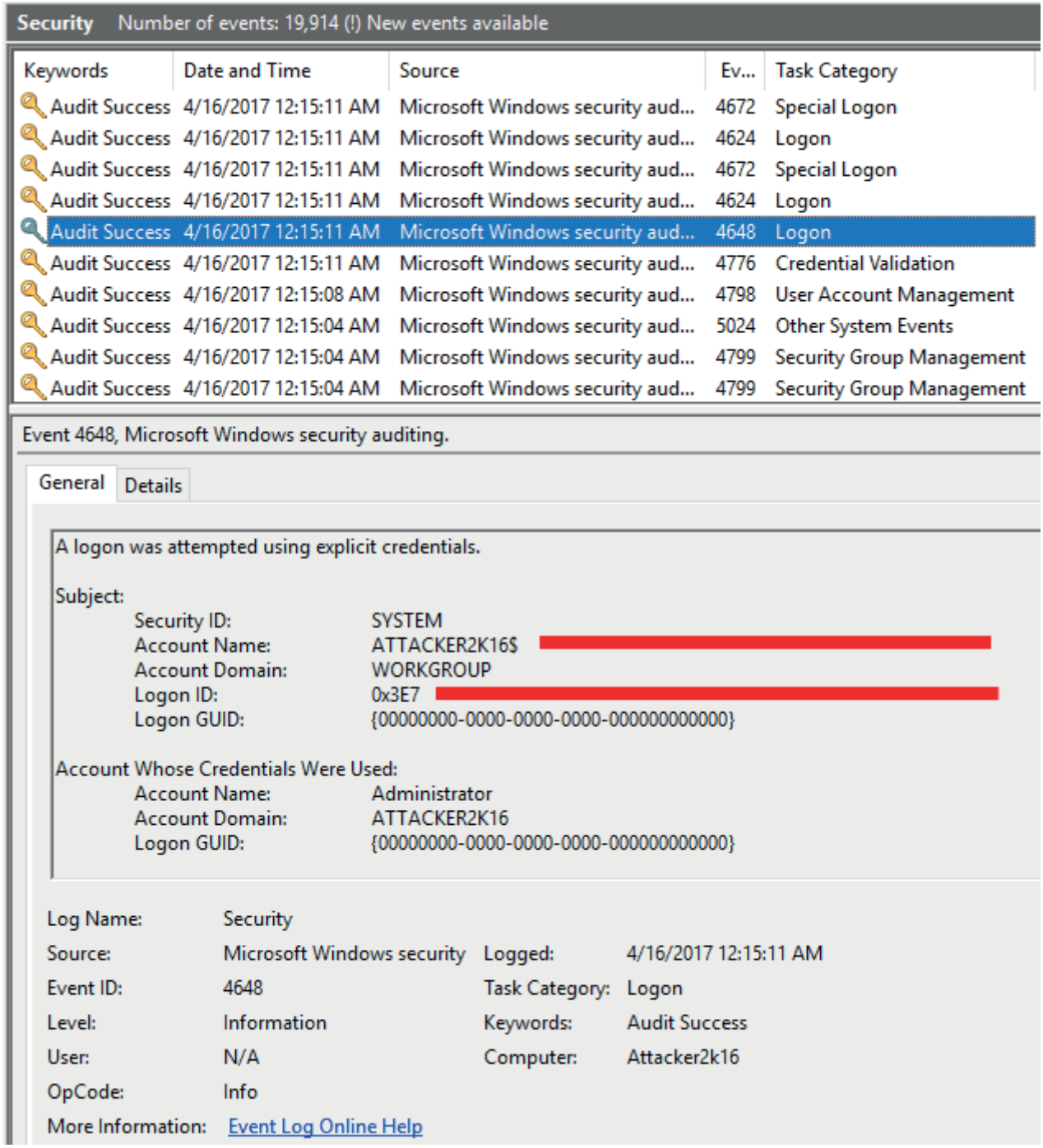


181. ábra

4776 esemény logja

Forrás: A szerző szerkesztése

Ezek után több, nekünk nem igazán kellő esemény következik, például a számítógép account próbál belépni.



182. ábra

4648 esemény logja

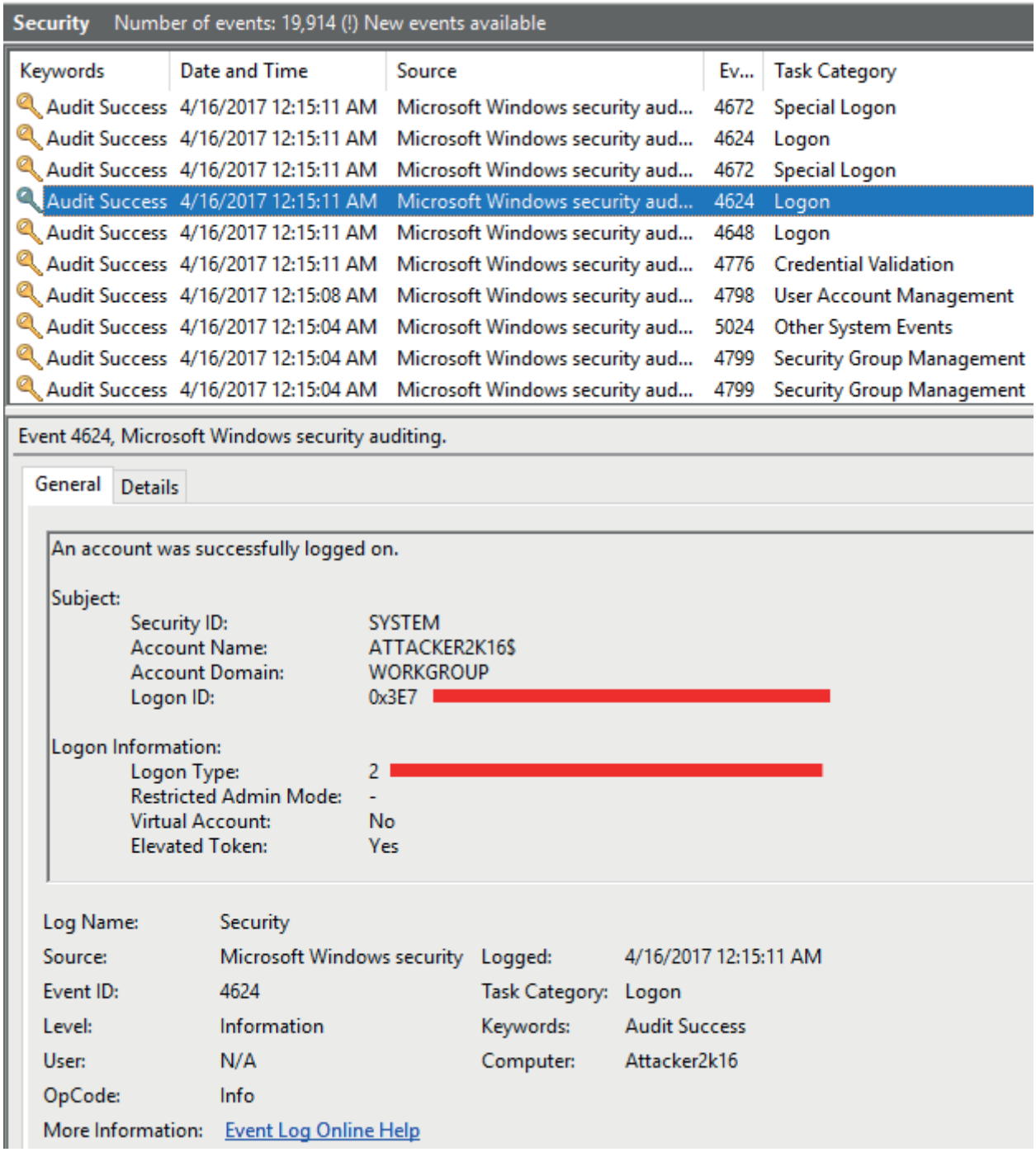
Forrás: A szerző szerkesztése

Sikerül is neki type 2, vagyis interactive logon. A többi logontípust lásd a 6. táblázatban!

6. táblázat
Logontípusok

logon type	Description
2	Interactive (logon at keyboard and screen of system)
3	Network (i.e. connection to shared folder on this computer from elsewhere on network)
4	Batch (i.e. scheduled task)
5	Service (Service startup)
7	Unlock (i.e. unnattended workstation with password protected screen saver)
8	NetworkCleartext (Logon with credentials sent in the clear text. Most often indicates a logon to IIS with "basic authentication")
9	NewCredentials such as with RunAs or mapping a network drive with alternate credentials. This logon type does not seem to show up in any events. If you want to track users attempting to logon with alternate credentials
10	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
11	CachedInteractive (logon with cached domain credentials such as when logging on to a laptop when away from the network)

Forrás: msdn.com

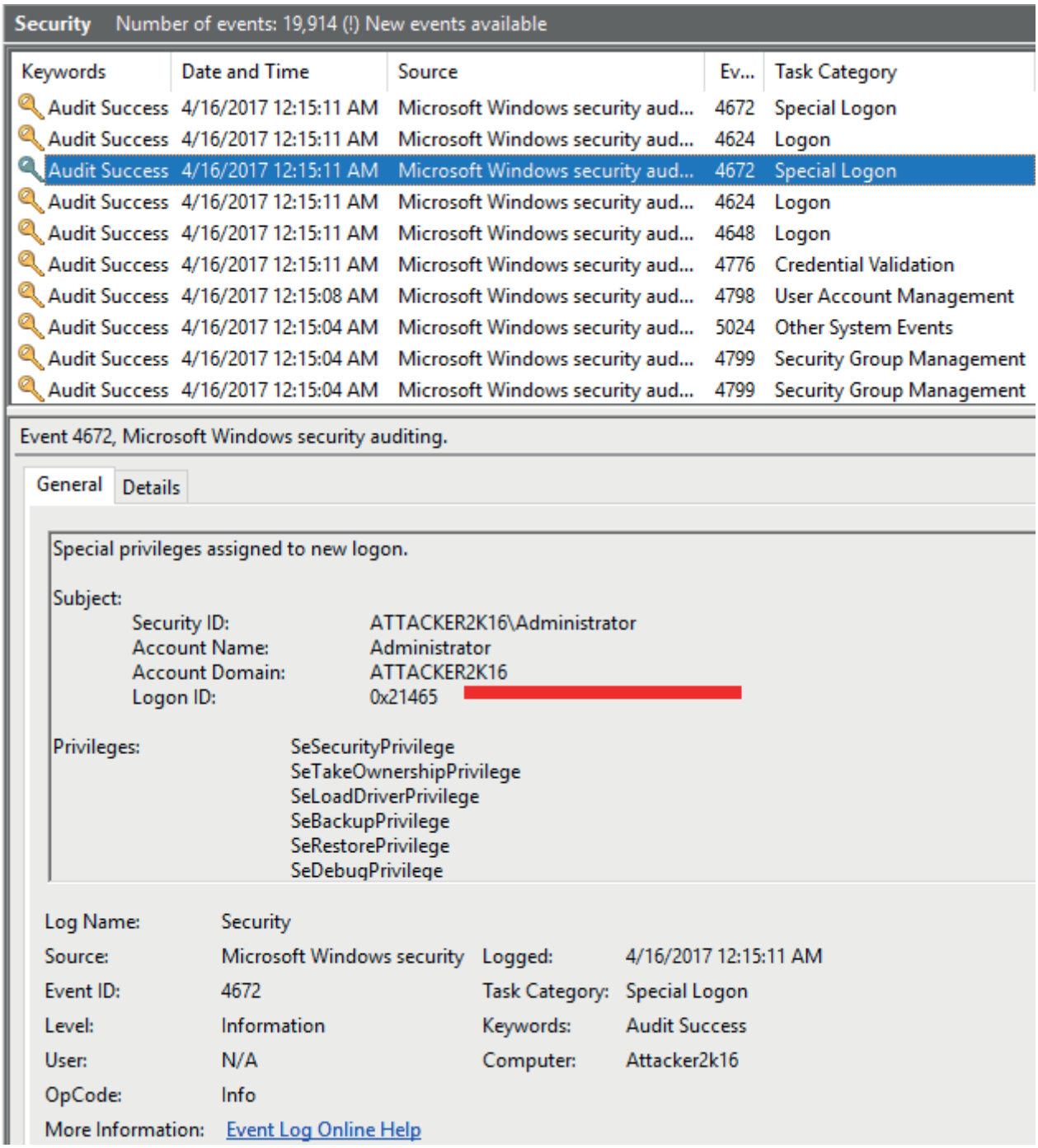


183. ábra

4624 esemény logja

Forrás: A szerző szerkesztése

Azután jön a számunkra leginkább lényeges 4672 Special logon, ahol látjuk, hogy az adminisztrátor tényleg belépett, és megkapta a speciális jogosultságait a logon id 0x21465; ezzel az értékkel találjuk majd meg a hozzá tartozó logoff eseményt.

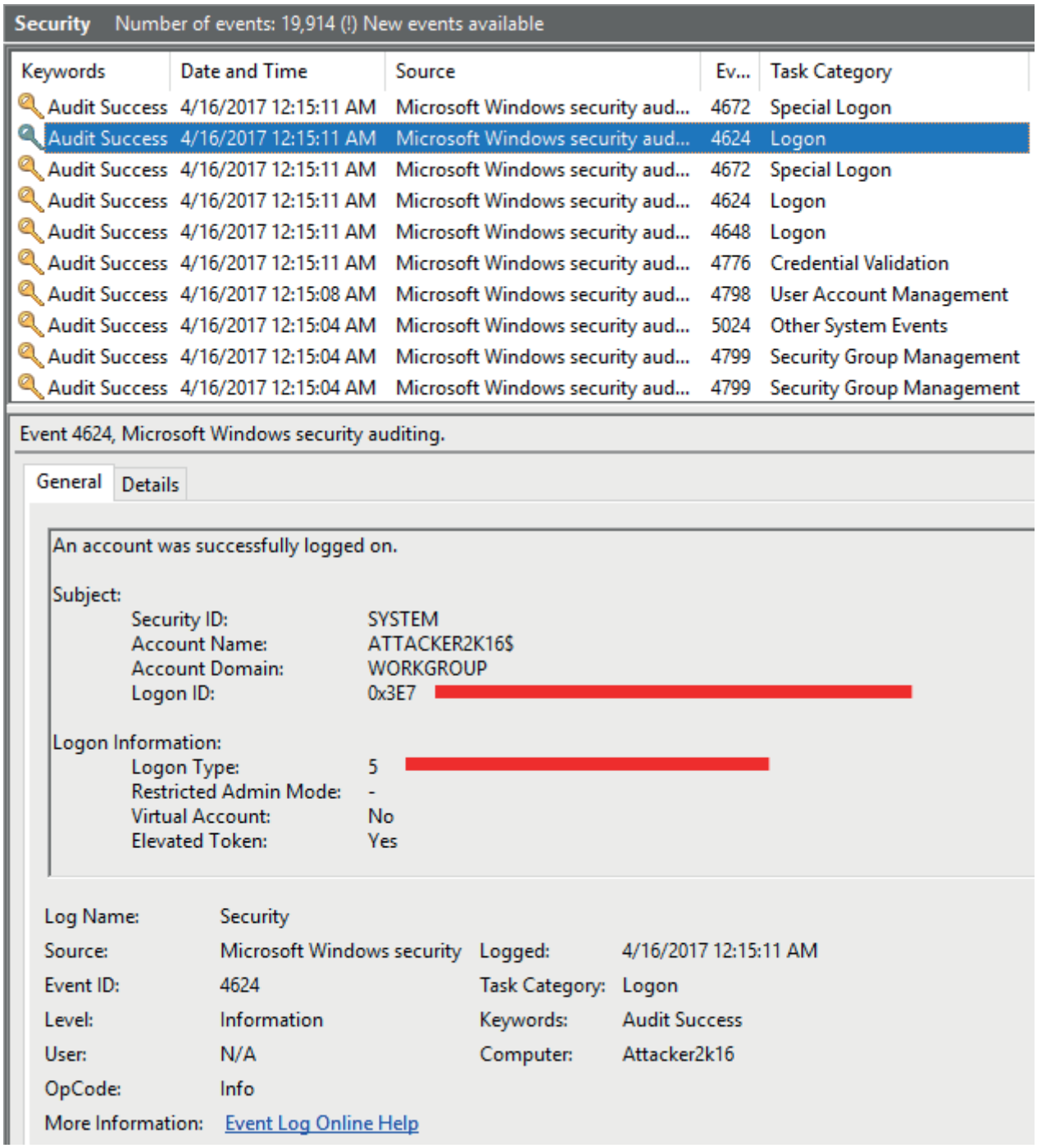


184. ábra

A 4672 Special logon

Forrás: A szerző szerkesztése

Azután még a computer account nevében indulnak servicek, és azok jelentkeznek be, lásd logon type 5.

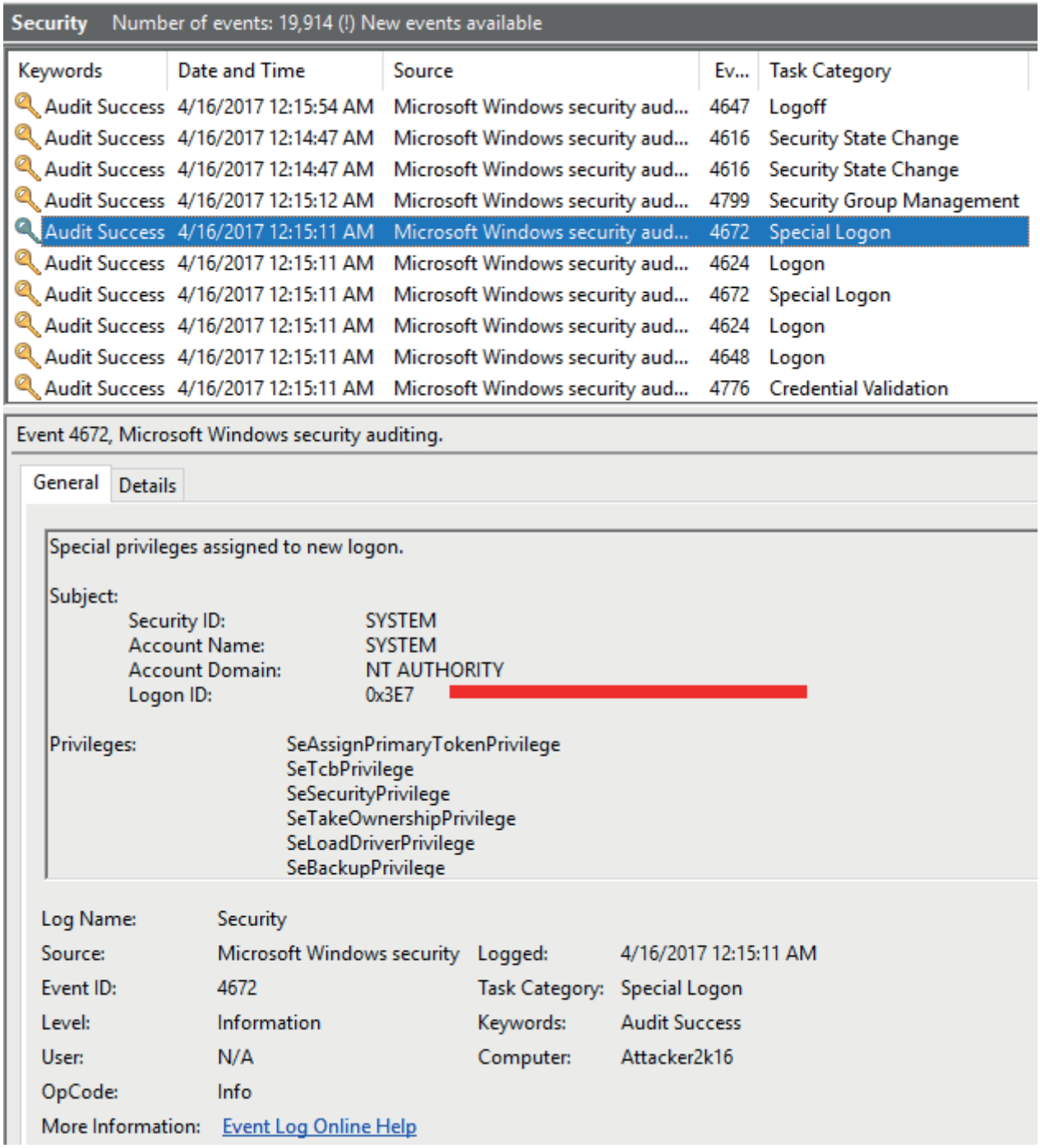


185. ábra

Logon Type 5

Forrás: A szerző szerkesztése

A servicenek is sikerül belépni, megkapta a saját speciális jogosultságait.



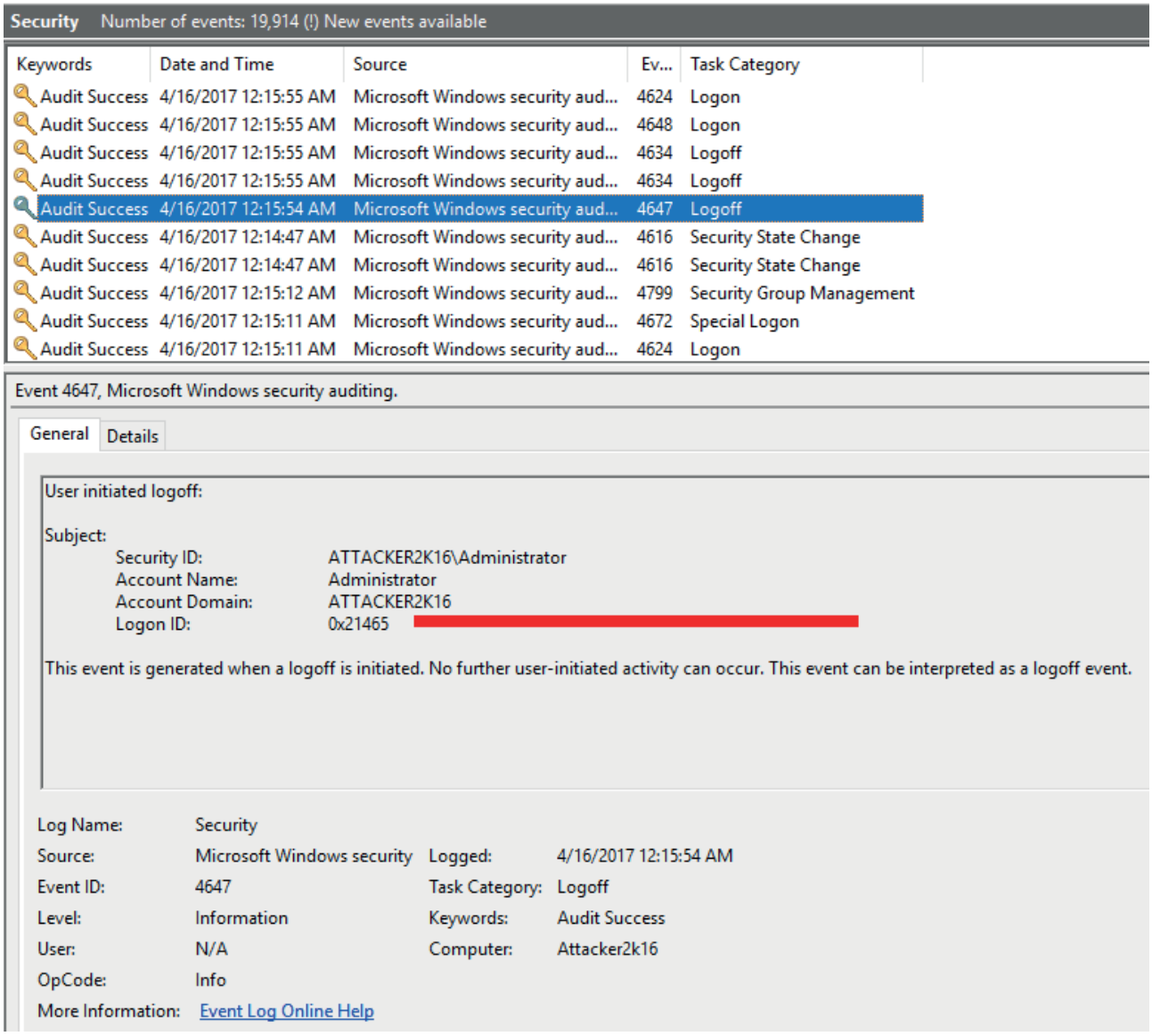
186. ábra

A service speciális jogosultságai

Forrás: A szerző szerkesztése

Ezután nézzük meg, ez hogyan párosítható össze a kilépési folyamattal!

Látjuk, hogy az adminisztrátor kilép, és a 0x21465 logon id-t most össze tudjuk vezetni a logonidőponttal, és a kettő alapján felírhatjuk, mettől meddig volt belépve a felhasználó. Közben persze ennek a felhasználónak a nevében processek indulhattak el, állhattak le, amik megzavarhatják a szép képet, nehezebbé teszik az összefésülést.

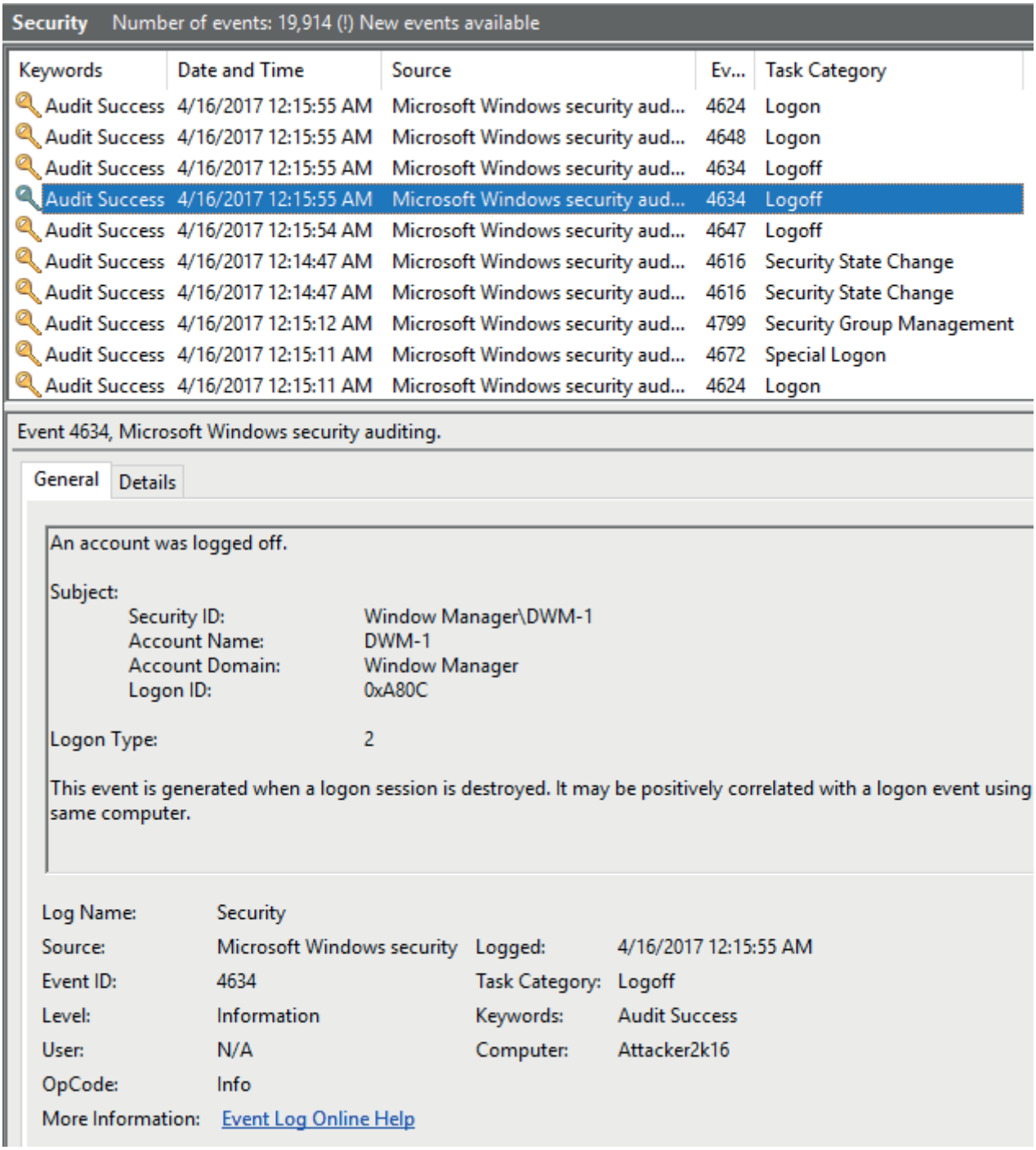


187. ábra

4647 esemény logja

Forrás: A szerző szerkesztése

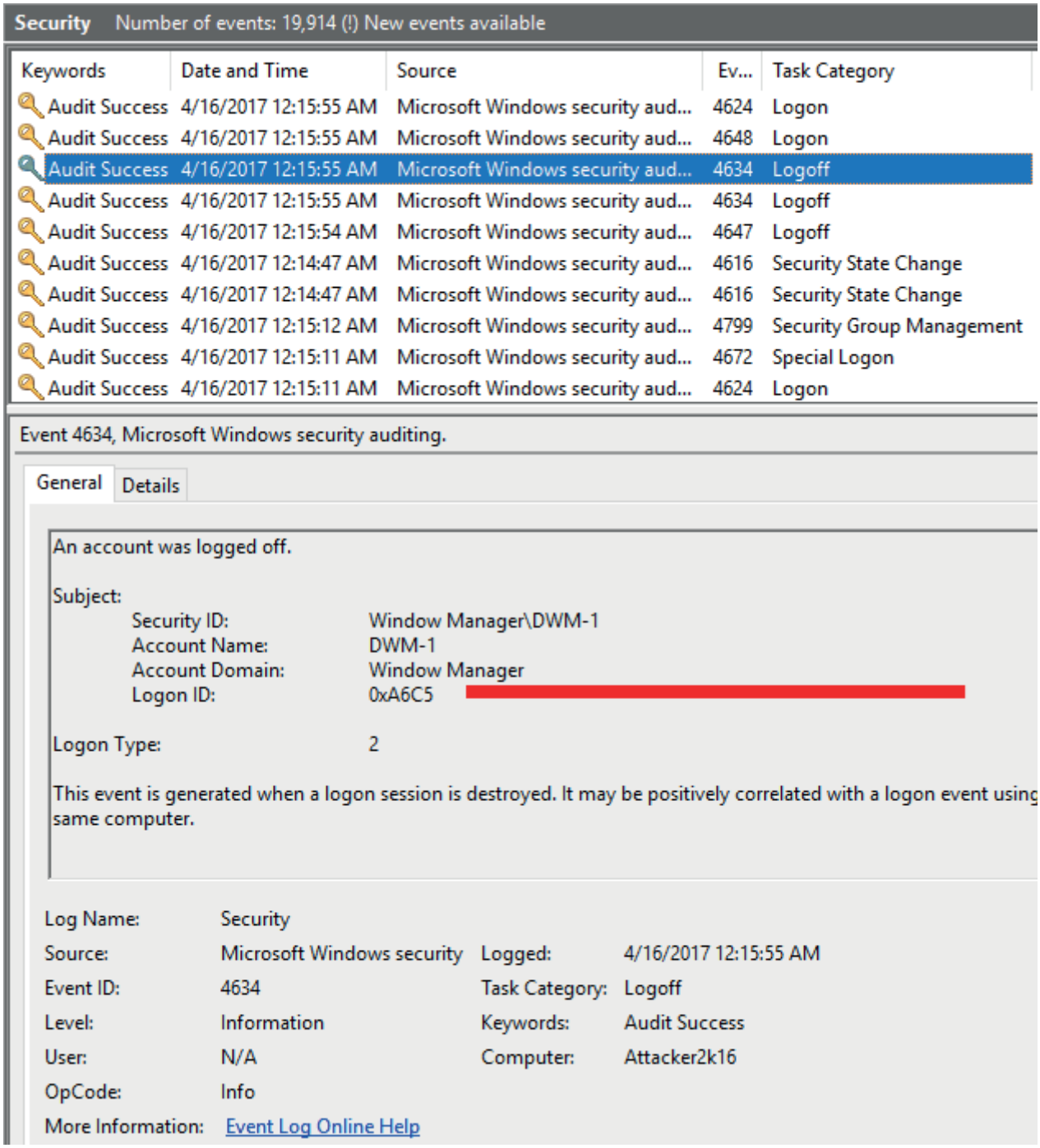
Azután különböző Windows processek is kilépnek még!



188. ábra

Kilépő windows processek

Forrás: A szerző szerkesztése



189. ábra

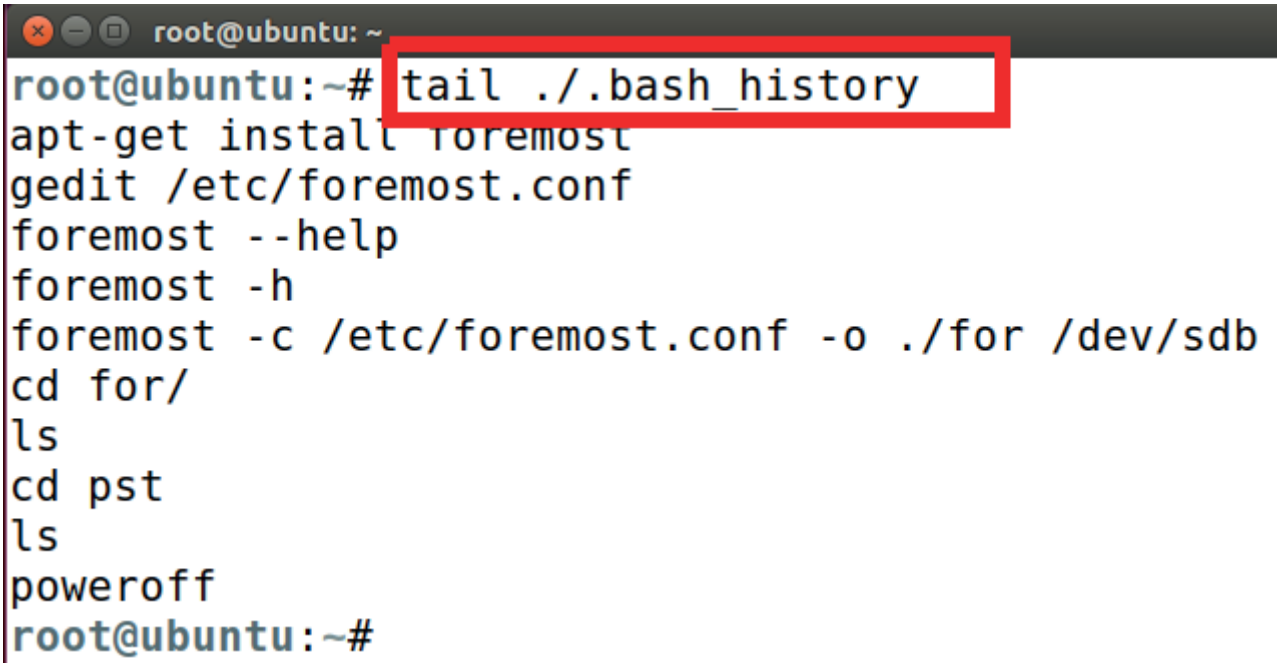
4634 esemény logja, session vége

Forrás: A szerző szerkesztése

9.7.2. A Linux operációs rendszer logjai

*Nix alapú operációs rendszerek alatt tipikusan szövegfájlokba kerülnek a logok, melyeket viszonylag könnyen elemezhetünk. A legfontosabb logok, amiket megnézünk a következők:

A user home folderekben található bash_history fájlok, ez tartalmazza az adott felhasználó által kiadott parancsokat.



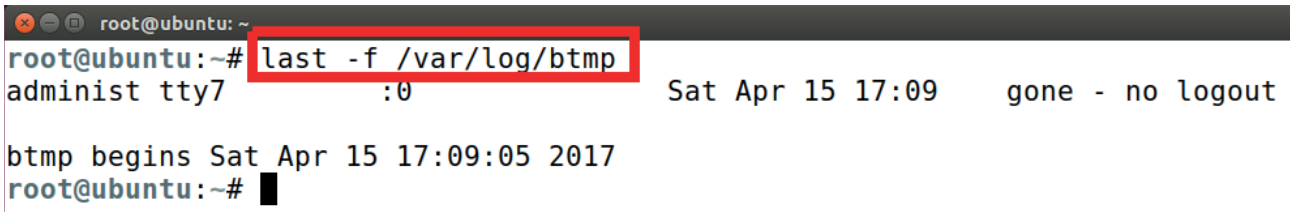
190. ábra

A bash_history fájlok

Forrás: A szerző szerkesztése

A /var/log alkönyvtárban találhatók az egyes alkalmazások logjai; itt a legkülönfélébb információk lehetnek, szintén szövegfájlokban tárolva. Például:

- btmp: a hibás bejelentkezések; ez egy bináris log, a last parancs segítségével írhatjuk ki olvasható formátumban.



191. ábra

A btmp bináris log

Forrás: A szerző szerkesztése

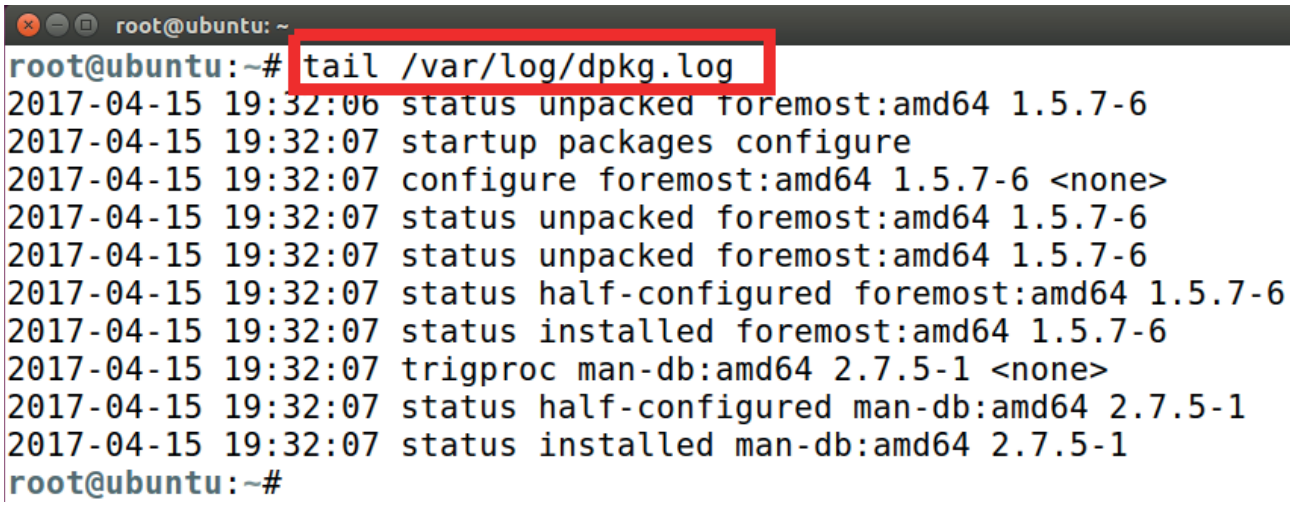
- dmesg: a deviceok, amelyeket a rendszerhez csatlakoztattak;
- auth.log: authentikációs folyamatok, milyen típusú authentikáció történt lokális vagy távoli, mit használtak jelszó, kerberos, ssh kulcs stb.;

192. ábra

Az auth.log

Forrás: A szerző szerkesztése

- dpkg.log: telepített, eltávolított csomagok; egy szövegfájl;

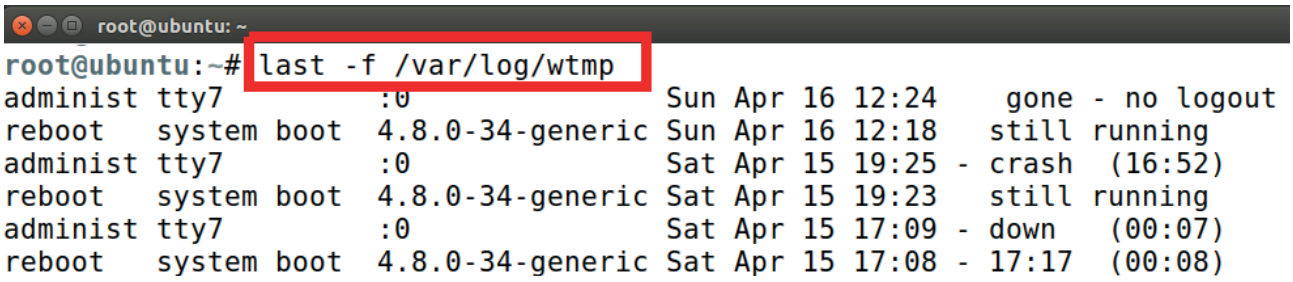


193. ábra

A dpkg.log

Forrás: A szerző szerkesztése

- cron: időzített jobokkal kapcsolatos információk;
- secure: szintén bejelentkezéssel és authentikációkkal kapcsolatos információk;
- wtmp: minden login és logout. Ez egy bináris fájl, a last parancs segítségével írhatjuk ki olvasható formátumban például: last -f /var/log/wtmp;



194. ábra

A wtmp bináris fájl

Forrás: A szerző szerkesztése

- utmp: egyes userek pillanatnyi bejelentkezési állapota. Ez egy bináris fájl, a last parancs segítségével írhatjuk ki olvasható formátumban például: last -f /var/log/utmp;
- httpd: apache logok szoktak ide kerülni, bár linux verzióknál változhat a hely;
- audit: audit daemon logjai;
- conman: remote console connectionnel kapcsolatos logok;
- xferlog: FTP atvitelek logjai.

9.8. Egyéb bizonyítékforrások

Sok minden lehet egyéb bizonyítékforrás, a teljesség igénye nélkül végignézünk párat, de itt mindig abban gondolkodjunk, hogy vizsgáljuk meg, hogy az adott operációs rendszerre milyen egyéb alkalmazások vannak telepítve, esetleg azok hol tárolhatnak még adatot.

9.8.1. Windows registry

Windows esetében egy nagyon gazdag információforrás lehet a registry. Itt a következő registry kulcsok lehetnek igazán fontosak:

Miket indítottak utoljára:

ntuser.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU;
ntuser.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU;
ntuser.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRULegacy;
ntuser.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist;
ntuser.dat\Software\Microsoft\Windows\ShellNoRoam\MUICache.

Legutóbbi dokumentumok:

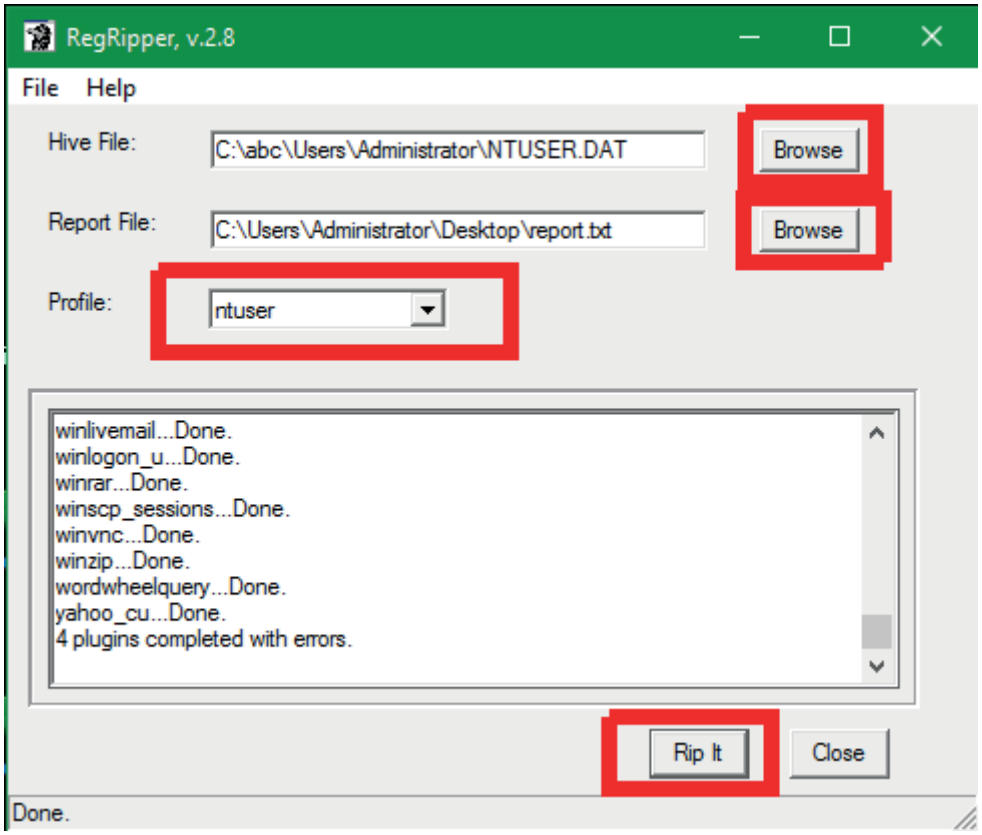
ntuser.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs;
ntuser.dat\Software\Microsoft\Windows\CurrentVersion\Applets\?*\Recent [File List];
ntuser.dat\Software\Adobe\?*\?*\AVGeneral\cRecentFiles\?*\tDIText;
ntuser.dat\Software\Microsoft\Office\?*\?*\Recent Files;
ntuser.dat\Software\Microsoft\Office\Office\?*\?*\File MRU;
ntuser.dat\Software\Microsoft\Office\Office\?*\?*\Place MRU.

Miket nyitottak meg utoljára bármilyen alkalmazásban, ami a windows open/save dialogbox-át használja:

ntuser.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU/?*/;
ntuser.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU/?*/.

Természetesen annak, hogy manuálisan keresgéljünk bizonyítékot a registryben, nem sok értelme van. Helyette registrykibontó eszközöket szoktunk használni. Az egyik eltrjedt ilyen alkalmazás a regripper, ami letölthető a regripper.wordpress.com weboldalról. A regripper egy perl-ben írt alkalmazás, de letölthető futtatható exe állományként is. A futó gép registryjét nem tudja használni, mert közvetlenül ez a program parsolja fel a bináris registry állományt, amik futó rendszer esetében fogottak. De ez nekünk nem megkötés, mert úgyis imagefájlokra szoktuk használni. Saját pluginekkel bővíthető is.

Amikor elindítjuk, válasszuk ki a hive fájlt, amiben keresni szeretnénk. Adjunk meg egy report fájlt, amibe a jelentést írja (egy sima text fájlt fogunk kapni). Válasszuk ki a profilt, hogy milyen fajta registry fájlt adtunk meg. Végül kattintsunk a Rip It gombra.

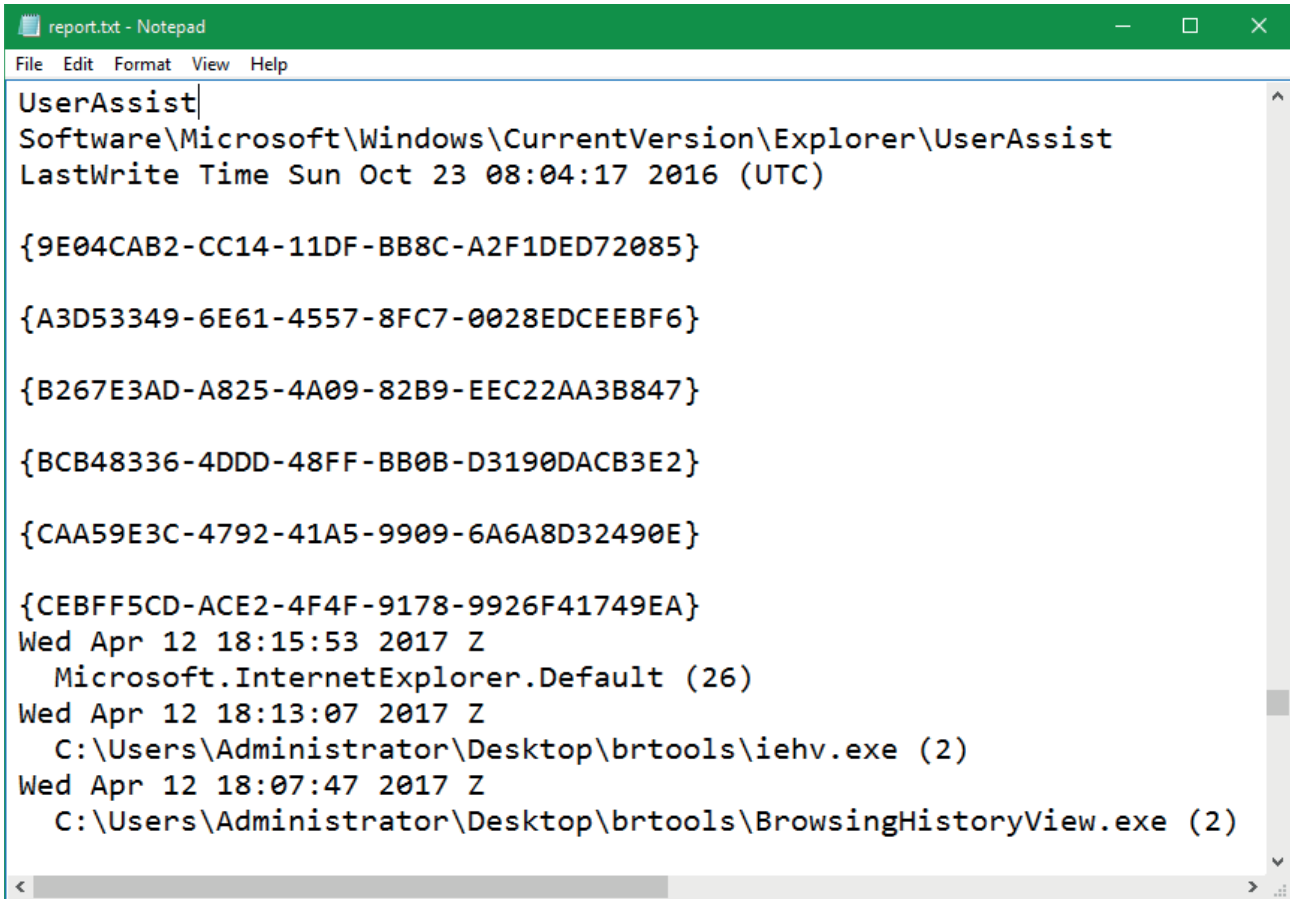


195. ábra

A regripper alkalmazás

Forrás: A szerző szerkesztése

A report fájlban rengeteg registrykulcs már olvasható formátumban mutatott adatai lesznek, például az egyik előbb említett kulcs, a userassist.



196. ábra

A userassist kulcs a reportfájlban

Forrás: A szerző szerkesztése

9.8.2. Windows prefetch fájlok

A registrynél kevésbé ismert, de nagyon fontos információforrások a prefetch fájlok. Ezek a c:\windows\prefetch alkönyvtárban találhatók. Amikor először elindítunk egy alkalmazást, akkor az operációs rendszer készít hozzá egy ilyen fájlt. A neve az elindított futtatható állomány neve, utána egy generált véletlen érték. Ebbe az állományba rögzíti, hogy milyen dll-eket töltött be az alkalmazás, és később, ha újra ezt az alkalmazást indítjuk, ennek segítségével előre tudja neki tölteni a dll-eket, innen ered a neve is. Innen olyan információkhoz juthatunk, hogy miket indítottak el ezen a gépen, mikor indították el utoljára, és milyen dll-eket használ. A prefetch fájlok bináris fájlok, tartalmukat prefetchnézegetővel tekinthetjük meg, például: www.nirsoft.net oldalról letölthető a win_prefetch_view alkalmazás.

Szerver operációs rendszereken ez alapból nincs bekapcsolva, mivel azokat tipikusan nem használjuk interaktív módon, csak limitált mennyiségű alkalmazást futtatunk rajtuk. Ha engedélyezni szeretnénk, használjuk a következő registry kulcsokat:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters\EnablePrefetcher

illetve:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Prefetcher\MaxPrefetchFiles

Felhasznált irodalom

Davidoff, Sherri – Ham, Jonathan (2012): *Network Forensics Tracking Hackers Through Cyberspace*. Prentice Hall.
Polstra, Philip (2015): *Linux Forensics*. Createspace Independent Publishing Platform.
FOR408 – Windows Forensic Analysis
Bunting, Steve (2007): *EnCE Study Guide*. Sybex – Serious skills.

JOGSZABÁLYTÁR[1]

A jegybanki információs rendszerhez elsődlegesen a Magyar Nemzeti Bank alapvető feladatai ellátása érdekében teljesítendő adatszolgáltatási kötelezettségekről szóló 23/2013. (XI. 6.) MNB rendelet
www.mnb.hu/letoltes/23-2013-xi-6-mnbrendelet.pdf

A kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól szóló 185/2015. (VII. 13.) kormányrendelet
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500185.kor

A közbeszerzésekről szóló 2015. évi CXLIII. törvény
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1500143.TV

A közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0400140.TV

A központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) kormányrendelet
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500186.kor

A központosított közbeszerzési rendszerről, valamint a központi beszerző szervezet feladat- és hatásköréről szóló 168/2004. (V. 25.) kormányrendelet
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0400168.KOR

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200166.tv

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013 (III. 8.) kormányrendelet
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1300065.kor

A Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről szóló 16/2013. (VIII. 30.) HM rendelet
www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2013/9.pdf

A Magyar Köztársaság Kormánya és a Németországi Szövetségi Köztársaság Kormánya között Budapesten, 1989. december 18-án aláírt légiközlekedési egyezmény kihirdetéséről szóló 86/1997. (V. 28.) kormányrendelet
http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99700086.KOR

A minősített adat védelméről szóló 2009. évi CLV. törvény
http://njt.hu/cgi_bin/njt_doc.cgi?docid=126195.323131

A nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1000157.tv

A Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásairól szóló 301/2013. (VII. 29.) kormányrendelet
http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300301.KOR&txtreferer=A1300050.TV

A Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről szóló 484/2013. (XII. 17.) kormányrendelet
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1300484.kor

A pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 42/2015. (III. 12.) kormányrendelet módosításáról szóló 157/2016. (VI. 13.) kormányrendelet
http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1600157.KOR&timeshift=ffffff4&txtreferer=00000001.TXT

[1] A letöltések dátuma: 2017. április 20.

A pénzügyi intézmények, a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről 535/2013. (XII. 30.) kormányrendelet
http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300535.KOR&txtreferer=A1300235.TV

A szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról szóló 83/2012. (IV. 21.) Kormányrendelet
http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200083.KOR&txtreferer=A1500042.BM

A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló Európai Parlament és a Tanács 95/46/EK irányelv
http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:31995L0046&from=HU

A támogatásból megvalósuló fejlesztések központi monitoringjáról és nyilvántartásáról szóló 60/2014. (III. 6.) kormányrendelet
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1400060.kor

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.323158

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre továbbá a biztonsági osztályba és a biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500041.bm

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet
http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300026.KIM

Az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól szóló 2013. évi CCXX. törvény
https://mkogy.jogtar.hu/?page=show&docid=a1300220.TV

Az állami szervek informatikai fejlesztéseinek koordinációjáról szóló 228/2016. (VII. 29.) kormányrendelet
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1600228.kor

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény
https://mkogy.jogtar.hu/?page=show&docid=a0100035.TV

Az elektronikus hírközlésről szóló 2003. évi C. törvény
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0300100.TV

Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) kormányrendelet
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1500187.KOR

Az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről szóló 42/2015. (VII. 15.) BM rendelet
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500042.bm

Az elektronikus ügyintézés részletes szabályairól szóló 85/2012. (IV. 21.) kormányrendelet
http://njt.hu/cgi_bin/njt_doc.cgi?docid=148205.295314

Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről
http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU

Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről
http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=HU

Az Európai Parlament és a Tanács 2002/58/EK (2002. július 12.) irányelve az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről
http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32002L0058&from=HU

Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10.) az Európai Hálózat és Információbiztonsági Ügynökség létrehozásáról
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:HU:HTML

Az Európai Parlament és a Tanács 526/2013/Eu rendelete (2013. május 21.) az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről
http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32013R0526&from=HU

Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér
http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52013JC0001&from=HU

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.322945

Egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről szóló 84/2012. (IV. 21.) kormányrendelet
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200084.kor

Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) kormányhatározat
http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf

FOGALOMTÁR

FOGALOM	DEFINÍCIÓ
(FIRST)CSIRT	Forum of Incident response and Security teams Számítógép biztonsági incidenskezelő csoport – Computer Security Incident Response Team
(TI) CSIRT	Trusted Introducer Számítógép biztonsági incidenskezelő csoport – Computer Security Incident Response Team
ACPI	Advanced Configuration and Power Interface, az APM felváltására készült energiagazdálkodási rendszer. Az utóbbival ellentétben nem a BIOS irányítja a folyamatokat, hanem az operációs rendszer.
ACT	Allied Command Transformation – Szövetséges Transzformációs Parancsnokság
adatbiztonság	Az adatok fizikai biztonságát szolgáló eljárások.
adatvédelem	A személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.
adatvédelmi incidens	A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.
advise	tanácsadás
AMT	intel-Active Management Technology
APWG	Anti Phishing Working Group
ASF	Advanced Streaming Format – a Microsoft által szabadalmazott digitális audio/digitális videócsomagoló (konténer), amit különösen a médiafolyamok továbbítására szántak.
ATP	Advanced Persistent Threat – fejlett támadás
BAH	Booz-Allen Hamilton
Bejelentés (logging)	A hívás és a hibakezelő rendszerben való rögzítést.
BfV	német Szövetségi Alkotmányvédelmi Hivatal (Bundesamt für Verfassungsschutz)
bizalmasság	Az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak, és ők is csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek annak felhasználásáról.
biztonsági esemény	Nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.
biztonsági esemény kezelése	Az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység.
Biztonságmenedzsment információs rendszere (security management information system)	Azon segédeszközök, adatok és információk összessége, amelyeket az információbiztonság-menedzsment támogatására használnak.
CA	Certification Authority – hitelesítésszolgáltató
CC	Common Criteria – közös követelmények
CCD CoE	Cooperative Cyber Defence Centre of Excellence – Kooperatív Kibervédelmi Kiválósági Központ
CDMA	Cyber Defence Management Authority
CDMB	Cyber Defence Management Board
CECSP	Közép-európai Kiberbiztonsági Platform (Central European Cyber Security Platform)
CERT	számítógépvészhelyzet-kezelő csoport – Computer Emergency Response Team
CERT/CC	számítógépvészhelyzet-kezelő csoport /koordinációs központ – Computer Emergency Response Team/ Coordination Center

FOGALOM	DEFINÍCIÓ
CERT/CC	CERT Competence Center
CFIA	Component Failure Impact Analysis
Címtár	Azonosítja és hitelesíti a szervezet felhasználóit, meghatározva alapvető jogosultságukat. A felhasználók és munkaállomások tevékenysége központilag korlátozható, a biztonsági házirendek központilag definiálhatók.
CIP CSIRT	A kritikus infrastruktúra védelméért felelős.
CIS	Center of Internet Security
CMS	Content Management System
COBIT	Control Objectives for Information and Related Technologies
Code of Practice	magatartási kódex
cookie	Egy információcsomag, amelyet a szerver küld a böngészőnek, majd a böngésző visszaküld a szervernek minden, a szerver felé irányított kérés alkalmával. Segíti a böngészést, biztonsági kockázata is van.
COSI	Az Európai Unió Belső Biztonsági Állandó Bizottsága
CRAMM	Risk Analysis and Management Method
CVSS	Common Vulnerability Scoring System
cyberbullying	elektronikus zaklatás
CSA	Cloud Security Alliance
CSIRT	Számítógép biztonsági incidenskezelő csoport – Computer Security Incident Response Team
CSIS	Stratégiai és Nemzetközi Tanulmányok Központ (Center for Strategic and International Studies
DDoS	Distributed Denial of Service – elosztott szolgáltatásmegtagadással járó támadás
Dead analízis	Lefoglalt anyagok (diskimage, memóriaimage, számítógép) analizálása
DENSEK projekt	Distributed Energy Security Knowledge
Disaster recovery site	Olyan része az informatikai rendszernek, mely attól fizikailag elkülönülő helyen üzemel, és az éles rendszer minden elemét és adatát tartalmazza.
DLP	Adatszivárgást megelőző eszköz
DMZ	A demilitarizált zóna a hálózat egy olyan része, amely mind az internet irányából, mind pedig a munkahelyi hálózatról csak speciális tűzfalszabályokon keresztül érhető el.
DNS szerver	Domain Name System
DoD	Department of Defense
DoS	Denial of Service – szolgáltatásmegtagadással járó támadás
dump file	Egy pillanatfelvétel az alkalmazásról.
EC3	European Cybercrime Centre – Europol Számítástechnikai Bűnözés Elleni Központ
EDR	Endpoint Detection and Response
EE-ISAC	European Energy – Information Sharing Analysis Centre
EMPACT Program	Európai Multidiszciplináris Platform a bűnügyi fenyegetés ellen – European Multidisciplinary Platform against Criminal Threats
ENISA	Európai Uniós Hálózat- és Információbiztonsági Ügynökség – European Union Agency for Network and Information Security
Eredendő ok (root cause)	Egy incidens vagy probléma mögöttes vagy eredeti oka.
Esemény (event)	Olyan állapotváltozás, amelynek jelentősége van egy konfigurációs elemben vagy az IT-szolgáltatás menedzsmentjében.
Észlelés (detection)	A kiterjesztett incidens-életciklus egy szakasza. Az észlelés hatására az incidens ismertté válik a szolgáltató számára.
Európai digitális menetrend	Célja, hogy a digitális technológia előnyei az európai polgárok és vállalkozások számára minél szélesebb körben elérhetők legyenek.
EUROPOL	Európai Rendőrségi Hivatal
failover	Az eszközöknek egy olyan felhasználása, amikor az informatikai rendszer azonos funkciójú elemeiből két vagy több példány folyamatosan működik, de egyidőben mindig csak egy érhető el.
FAIR	Fejlesztéspolitikai Adatbázis és Információs Rendszer
FancyBear	Hackercsoport
FI-ISAC	European Financial Institutes – Information Sharing and Analysis Centre

FOGALOM	DEFINÍCIÓ
forensics	A bizonyítékokat olyan minőségben, és azoknak az alapelveknek a betartásával gyűjtsük össze és analizáljuk, amik garantálják, hogy akár egy bírósági tárgyaláson is elfogadhatók lesznek.
Forrótartalék (hot start, hot standby)	Olyan létesítmény, amelyben az eszközök azonnal képesek a szoftverek archivált adat feltöltésére és futtatására.
FTA	Fault Tree Analysis – Hibafaelemzés
FTK	The Forensic Toolkit képes többek között disk, és memória imagelésre is.
GAO	U.S. Government Accountability Office
GDPR	Európai Unió Általános Adatvédelmi Rendelete – General Data Protection Regulation
GovCERT	Kormányzati Eseménykezelő Központ
GPT	Guid Partition Table – partícióeloszlás-táblázat
Hálózati szegmentáció	A különböző funkciójú infrastruktúraelemeket egymástól hálózati eszközök segítségével elválasztják.
hash függvény	Olyan, informatikában használt eljárások, amelyekkel bármilyen hosszúságú adatot adott hosszúságra képezhetünk le.
Hiba (error/fault)	Tervezési hiányosság vagy helytelen működés, amely meghibásodást okoz egy vagy több konfigurációelemben vagy IT-szolgáltatásban.
Hidegtartalék (cold start, cold standby)	Olyan hordozható vagy helyhez kötött létesítmény, amelyben alapinfrastruktúrával (kábelezés, áramellátás) rendelkező számítógépközpont van.
Hívás (call)	Telefonhívás a felhasználótól az ügyfélszolgálatra.
HSAC	Homeland Security Advisory Council–Belbiztonsági tanácsadó testület (USA)
Hun-CERT	Internet Szolgáltatók Tanácsa (ISZT) tagjainak CERT-je.
Iaas	azonnal elérhető számítási infrastruktúra
IBSZ	informatikai biztonsági szabályzat
IDC	International Data Corporation
IDF	behatolásdetektáló rendszer
incidens	Egy IT-szolgáltatás be nem tervezett megszakadása, vagy minőségének csökkenése.
Információbiztonság-menedzsment (information security management)	Ez a folyamat felelős azért, hogy egy szervezet eszközeinek, információinak, adatainak és IT-szolgáltatásainak bizalmassága, integritása és rendelkezésre állása megfeleljen a megállapodott üzleti igényeknek.
IoC	Indicator of Compromise
IPS	behatolásmegelőző rendszer
IPS/IDS rendszer	A külső támadások elleni védelem eszközei, a forgalom folyamatos elemzését végzik, és szükség esetén riasztani képesek az adott folyamat letiltása érdekében.
IRT	incidenskezelő csapat
ISACA	Információ rendszer menedzserek és ellenőrök nemzetközi szakmai szervezete
Ismert hiba (known error)	Olyan probléma, amelynek van dokumentált eredendő oka és megkerülő megoldása.
ITGI	IT Governance Institute
ITIL	nemzetközi szabvány – informatikai rendszerek üzemeltetésére és fejlesztésére vonatkozó ajánlás, módszertan
ITIL	Information Technology Infrastructure Library
ITILv3	legfirssebb szabányverzió
IWWN	Nemzetközi CSIRT közösség
katasztrófa (disaster)	Olyan hirtelen, nem tervezett, szerencsétlen esemény, amely jelentős kárt vagy veszteséget okoz.
Katasztrófa-elhárítási Terv (Disaster Recovery Plan – DRP)	Azoknak az eljárásoknak a gyűjteménye, amelyek alapján egy szervezet képes a káresemények következtében kiesett szolgáltatásait a normál működési szintre visszaállítani.
KEF	Közbeszerzési és Ellátási Főigazgatóság
kibertér	A számítógéprendszerek és -hálózatok által alkotott metaforikus tér, amelyben elektronikus adatok tárolódnak, és online adatforgalom, valamint kommunikáció zajlik.
KNBSZ	Katonai Nemzetbiztonsági Szolgálat

FOGALOM	DEFINÍCIÓ
különleges személyes adat	A faji eredetre, a nemzetiségi hovatartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdekképviseleti szervezeti tagságra, a szexuális életre, az egészségi állapotra, valamint a kóros szenvedélyre vonatkozó és a bűnügyi személyes adat.
live analízis	a futó számítógépet vizsgálata
LMS	Learning Management System
load ballancing	Az eszközöknek egy olyan felhasználása, amikor az informatikai rendszer azonos funkciójú elemeiből két vagy több példány folyamatosan működik a rendszerben, és folyamatosan elérhetők a felhasználók számára.
LRLIBEK	Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ
malware	Rosszindulatú program
Meghibásodás (failure)	Annak a képességnek az elvesztése, hogy valami előírás szerint működjön, vagy a kívánt eredmény előálljon.
Megkerülő megoldás (workaround)	Olyan incidens vagy probléma hatásának csökkentése vagy kiküszöbölése, amelyre teljes megoldás még nincs (például egy meghibásodott konfigurációelem újraindítása).
Megoldás (resolution)	Intézkedés egy incidens vagy probléma eredendő okának kijavítására, vagy egy megkerülő megoldás megvalósítására.
Microsoft Event log	microsoft naplózási protokoll
MILCERT	honvédelmi/katonai CERT
Minőség (quality)	Egy termék, szolgáltatás vagy folyamat képessége arra vonatkozóan, hogy a tervezett értéket nyújtsa (például egy hardverkomponenst jó minőségűnek kell tekinteni, ha az az elvárások szerint működik, és nyújtja az elvárt megbízhatóságot).
MOF	Microsoft Operations Framework
MTA SZTAKI	Magyar Tudományos Akadémia Számítástechnikai és Automatizálási Kutatóintézet
Működésfolytonossági Terv (MFT), (Business Continiuty Plan – BCP)	Azoknak az információknak és eljárásoknak a gyűjteménye, amelyek alapján egy szervezet képes váratlan káreseményekre hatékonyan reagálni, és kritikus üzleti folyamatait egy elfogadható szinten fenntartani. MFT-nek nevezik azt a keretrendszert, amely átfogja a működésfolytonosság tervezési, megvalósítási és ellenőrzési fázisait.
NAC	Network Access Control – Hálózati hozzáférés-felügyelet
NAIH	Nemzeti Adatvédelmi és Információszabadság Hatóság
NCSC	Nemzeti Kiberbiztonsági Központok – National cyber Security Center
NEIH	Nemzeti Elektronikus Információbiztonsági Hatóságra
nemzeti adatvagyon	A Magyarországgal kapcsolatos vagy a tulajdonában lévő, hozzáférhető adatok összesége.
NIIF-CSIRT	Nemzeti Információs Infrastruktúra Fejlesztés
NIIFI-CSIRT	Nemzeti Információs Infrastruktúra Fejlesztési (NIIF) Intézet incidenskezelési csoportja.
NIST	Nemzeti Szabvány és Technológiai Intézete – National Institute of Standards and Technology
NKI	Nemzeti Kibervédelmi Intézet
NMHH	Nemzeti Média- és Hírközlési Hatóság
NMHH-OIHF	Országos Informatikai és Hírközlési Főügyelettel
NMSDB	Network Management System Database
nulladik napi fenyegetés	Egy biztonsági fenyegetés, amely valamely számítógépes alkalmazás olyan sebezhetőségét használja ki, ami még nem került nyilvánosságra, a szoftver fejlesztője nem tud róla, vagy nem érhető még el azt foltozó biztonsági javítás.
OECD	Gazdasági Együttműködési és Fejlesztési Szervezet
ORFK NEBEK	Országos Rendőr-főkapitányság Nemzetközi Bűnügyi Együttműködési Központ
OSCE	Organization for Security and Co-operation in Europe – Európai Biztonsági és Együttműködési Szervezet (EBESZ)
PaaS	azonnal elérhető platform
PDCA elv	Plan-Do-Check-Act – tervezés-végrehajtás-ellenőrzés-beavatkozás
PKI	Public key infrastructure – közöségi kulcs infrastruktúra
PreDeCo elv	Preventive-Detective-Corrective – Megelőzés-felderítés-korrigálás
Problémamenedzsment (Problem Management)	A szolgáltatás üzemképtelenségének minimalizálása a fő célja.
proxy	Helyetesítő/kiváltó
ransomware	zsarolóvírus

FOGALOM	DEFINÍCIÓ
Rendelkezésre állás	Az elektronikus információs rendszerek az arra jogosult személy számára elérhetők, és az abban kezelt adatok felhasználhatók.
reporting	gyakorlatok megosztása
rootkit	Olyan szoftvereszköz, amely segítségével egy cracker könnyen visszatérhet a „tett színhelyére”, ha már korábban beférkőzött a rendszerbe, hogy bizalmas adatokat gyűjtsön a fertőzött számítógépről.
SaaS	azonnal elérhető szoftver
sandbox	Olyan ellenőrzött – valós világhoz közeli – informatikai környezet, ahol megfigyelhető egy állomány futtatása során annak tevékenysége, úgy, hogy az ne jelentsen veszélyt a teljes informatikai rendszerre.
SECaaS	azonnal elérhető biztonsági szolgáltatás
SEM	Security Event Management – Biztonsági eseménykezelő
SERT	Security Emergency Response Team – Sürgősségi reagáló biztonsági csapat
Sértetlenség	Az adat tartalma és tulajdonságai az adattal szemben felállított követelményekkel megegyeznek, az adat az elvárt forrásból származik, azaz hiteles és származása ellenőrizhető.
SIEM	Security Information and Event Management – Biztonsági információ- és eseménykezelő csoport
SIM	Security Information Management – Biztonsági információkezelés
SLA	Service Level Agreement – Szolgáltatásiszint-megállapodás
SNMP	Simple Network Management Protocol – Egyszerű hálózatkezelő protokoll
SOA	Szolgáltatásorientált architektúra (Service Oriented Architecture)
SOAR	Biztonsági eseménykezelő rendszer
SOC	Biztonsági Üzemeltetési Központok – Secrity Operation központok
social engineering	Támadási forma, ahol a hozzáféréssel rendelkezőket zsarolják vagy befolyásolják, esetleg bizalmukba férkőzve kihasználják hiszékenységüket.
SSO	Single Sign-On – egyszeri bejelentkezési módszer
Stuxnet	Annak a rosszindulatú programnak a neve, amelyet célzottan csak az iráni urándusító létesítmény ellen terveztek, és amely csak azt támadta meg, annak ellenére, hogy több százezer számítógépen is megtalálták később.
SWOT analízis	A stratégiaalkotás folyamatának egyik lépése (Strengths–erősségek Weaknesses–gyengeségek Opportunities–lehetőségek Threats–veszélyek).
SYN Flood	elárasztásos támadás
syslog	linux naplózási protokoll
Szolgáltatás helyreállítása (restoration of service)	Intézkedés egy IT-szolgáltatás javítása és visszaállítása utáni visszaadásáról a felhasználóknak.
Szolgáltatásstratégia (Service Strategy)	A folyamat azonosítja azokat a piaci lehetőségeket, amelyeket új szolgáltatások bevezetésével ki lehetne használni.
Szolgáltatástervezés (Service Design)	A folyamat eredményeként projektterv készül az előző lépésben keletkezett stratégia által felvázolt szolgáltatás konkrét megvalósítására.
TARANSITS	Egy európai projekt, amelynek célja az új CSIRT-ek létrehozásának és a már működő CSIRT-ek bővítésének, fejlesztésének támogatása speciális tanfolyamok által.
TCO	Total Cost of Ownership – Teljes Bekerülési Érték
TI	fenyegetettségi információszolgáltatás
Tivoli Security Policy Manager	Leválasztja a biztonsági irányelveket az alkalmazásokról, lehetővé téve az alkalmazásjogosítványok központosítását és leegyszerűsítését, valamint az adathozzáférés részletes szabályozását.
TPM	Trusted Platform Module
Tűzfal	A külső támadások ellen védik a szervezeti infrastruktúra elemeit.
Üzleti hatáselemzés (Business Impact Analysis – BIA)	Eljárás, amely során a szervezet meghatározza a kritikus üzleti folyamatok megszakadásának következményeit és a normál működési állapotra való visszaállás elvárásait.
Üzletmenetfolytonosság-menedzsment (Business Continuity Management – BCM)	Az a folyamat, melynek során egy szervezet felkészül a kritikus üzleti folyamatok megszakadására, vagy kiesése esetén a folyamatok visszaállítására.

FOGALOM	DEFINÍCIÓ
vis major	váratlan, nem befolyásolható esemény
volatility	változékonyság
volatility	memória dump analizáló eszköz
VPN	virtual private network – virtuális magánhálózat
warning	riasztás
WARP	Warning, Advise and Reporting Points
WBEM	Web-Based Enterprise Management
WMI	Windows Management Interface
Worm attack	féregtámadás

A Nemzeti Közszolgálati Egyetem kiadványa.

Nordex Nonprofit Kft. – Dialóg Campus Kiadó • www.dialogcampus.hu • www.uni-nke.hu • 1083 Budapest, Ludovika tér 2. • Telefon: 06 (30) 426 61 16 • E-mail: kiado@uni-nke.hu • A kiadásért felel: Petró Ildikó ügyvezető • Kiadói szerkesztő: Szarvas Melinda • Felelős szerkesztő: Karácsony Fanni • Tördelőszerkesztő: Stubnya Tibor

ISBN 978-615-5764-99-8 (PDF)
ISBN 978-615-5845-00-0 (EPUB)

A kiadvány a KÖFOP-2.1.1-VEKOP-15-2016-00001 „A közszolgáltatás komplex kompetencia, életpálya-program és oktatás technológiai fejlesztése” című projekt keretében jelent meg.